A Go-to-Market Strategy

Promoting Private Sector Solutions to the Threat of Proliferation

By Nate Olson
with Brian Finlay and Esha Mufti

The Stimson Center
April 2013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
APR 2013		**00-00-2013 to 00-00-2013**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
A Go-to-Market Strategy: Promoting Private Sector Solutions to the Threat of Proliferation	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **The Stimson Center,1111 19th Street NW,Twelfth Floor,Washington,DC,20036**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**46**	

Acknowledgements

Stimson is most grateful to all of the project's industry and government participants, whose observations, assessments, and recommendations formed the basis for this report. Our industry interlocutors, in particular, deserve special thanks for being exceptionally generous with their time and ideas.

We also wish to extend sincere appreciation to Alex Georgieff, Alex Davis, and Natasha John of Stimson for their excellent research assistance. Finally, we thank our Stimson colleague Debra Decker for her input on insurance and risk management topics.

This material is made possible in part by support from the Project on Advanced Systems and Concepts for Countering Weapons of Mass Destruction (PASCC), Center on Contemporary Conflict, Naval Postgraduate School, under Grant No. N00244-12-1-0034. PASCC is supported by the Defense Threat Reduction Agency (DTRA).

Contents

Executive Summary

The interconnectivity, complexity, and fluidity of global commerce suggest that the ability of governments to control the proliferation of dangerous technologies is diminishing—at the very moment proliferation and other transnational criminal challenges are increasing. Privatization, outsourcing, global industrial development, and the migration of many business activities to an electronic medium are pushing sensitive items into more hands and decreasing the capacity of even well-resourced and well-intentioned governments to regulate these activities. A wide array of private sector companies—from dual-use technology innovators and manufacturers, to shipping firms, investors, and the insurance and banking industries—play a role in the movement of dangerous materials, limiting direct government control over the means of production and causing them, potentially, to contribute to the proliferation of weapons of mass destruction (WMD), knowingly or otherwise.

While government regulation will remain the central element in preventing WMD proliferation and combatting other forms of transnational criminal activity, in some cases, governments are approaching the practical limits of legal restrictions and criminal enforcement of the rules. Developing government and private sector partnerships is widely recognized to be a critical component for successful nonproliferation and counter-trafficking efforts; however, neither the government nor the expert community has systematically developed practical collaborations that go beyond threats of additional regulation. While not a panacea, self-regulation incented by the market is an under-leveraged tool in current prevention efforts.

Introduction

The interconnectivity, complexity, and fluidity of global commerce suggest that the ability of governments to control the proliferation of dangerous technologies across national boundaries is diminishing—at the very moment proliferation and other transnational criminal challenges are increasing. This trend owes to three interdependent facts: First, proliferation threats are evolving because of the globalized diffusion of WMD capacities which are themselves rooted in, and facilitated by, a growing network of private sector actors. Second, this new reality necessitates renewed attention on building innovative new partnerships with industry if our efforts to prevent proliferation are to succeed. And finally, while the means of WMD production were once the exclusive purview of governments, the privatization of those capacities has led to a growing convergence between the threat of WMD proliferation and a broad array of transnational threats. These facts may lead security analysts to despair. Viewed more objectively and expansively, though, they open up new opportunities to modernize our preventive toolkit to more sustainably, effectively, and efficiently address a broad array of international trafficking and proliferation threats.

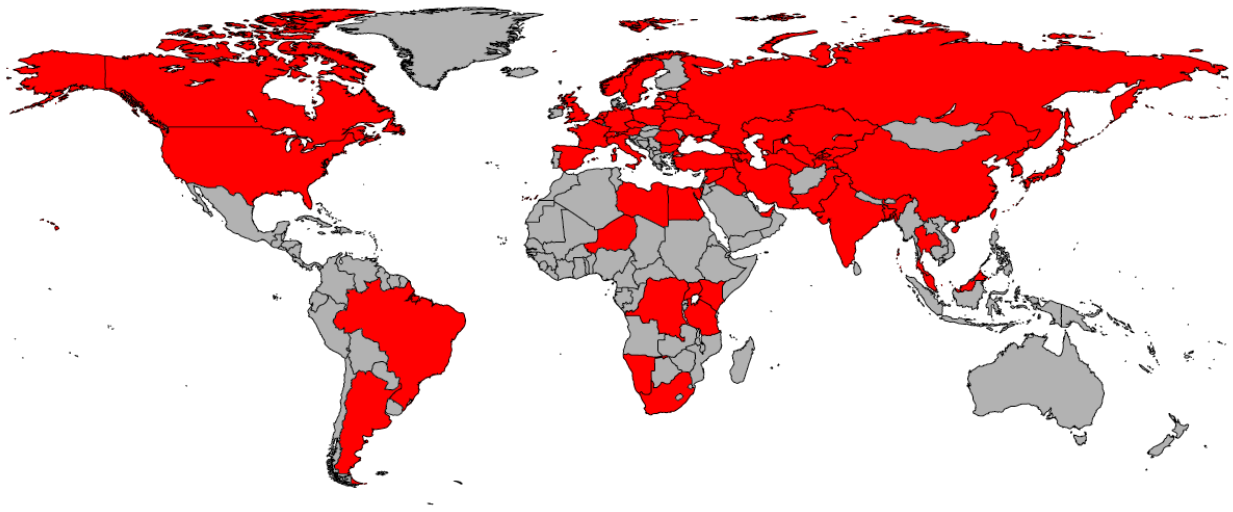
The Evolving Proliferation Threat and the Growing Role of Private Industry

Over the past quarter century, globalization has revolutionized the international system. Several decades of cascading liberalization in trade and capital markets has greatly expanded the availability of sophisticated materials, technologies, and expertise. It has meant greater prosperity for billions of people and enabled development of a global physical and informational infrastructure that has further reinforced economic integration. But it also has empowered criminals and terrorists at an entirely different scale. Indeed, while development specialists rightly celebrate this trend, international security specialists view globalization's associated transfer of technologies—including sensitive dual use technologies to regions with a vacuum of regulatory and enforcement capacity—with grave concern.

As globalization has democratized access to technology, moreover, the private sector has increasingly been at the vanguard of this movement. Industry is, today, the dual-use technology innovator, the weapons manufacturer, the air or seaborne carrier, the financial investor, or the insurance underwriter. As such, an array of companies—from technology innovators, high-technology fabricators and manufacturers, private investors, financial and insurance firms, and a rapidly-expanding supply chain industry—has also contributed, knowingly or unknowingly, to the illicit trade in dangerous products, materials, and technologies, including dual-use WMD items.

Figure 1 indicates the number of states whose territories have been used or whose firms were complicit in International Atomic Energy Agency's (IAEA) documented incidents of materials trafficking. The Figure suggests that even the most rigorous attempts at regulation can be circumvented by a committed proliferator and the growing obsolescence of the state-centric means of denial. Almost always, these incidents have involved an array of private sector entities whose motivations are legitimate growth and profit.

FIGURE 1
THE MODERN PROLIFERATION SUPPLY CHAIN



Regardless of intent or foreknowledge, countries in red have been implicated in the AQ Khan Affair and/or listed in the IAEA Illicit Trafficking Database.[1]

One need not look beyond the 2005 discovery of an American-made computer circuit in an unexploded roadside bomb in Iraq to realize the perils of technology diffusion. In this case, radio frequency modules produced by a Minnesota company were sold to middlemen in Singapore, forwarded to Iran by air freight through a third country, then smuggled across the border into Iraq. The consequences of similar transactions in support of a WMD program, as with the AQ Khan Affair, are incalculable.

The case of the German multinational manufacturing firm Oerlikon Leybold also reflects the evolving challenge. In 1991, while searching a remote outpost in the Iraqi desert, UN weapons inspectors stumbled upon a small number of vacuum pumps supplied by Oerlikon Leybold Vacuum. At the time, none of the items discovered was listed in any national or multilateral export control regime. But upon closer study, the inspectors realized that the vacuum pump was attached to a cyclotron, which can be used to enrich uranium through electromagnetic isotope separation.

Thus, Oerlikon and its competitors had knowingly—though innocently—supplied the pumps to the Iraqi government and unwittingly advanced its nuclear weapons program. As news of this spread, the damage to the Oerlikon brand prompted the company to re-think its fulfillment of a growing number of suspicious requests for technology. The incident also highlighted the ease with which proliferators can exploit legitimate companies to obtain weapons technologies, the inability of existing measures to always contain this growing threat, and the serious consequences that illicit networks may have on both legitimate business operations and global security.[2]

---

[1] International Atomic Energy Agency, "Illicit Trafficking Database" (now technically the "Incident and Trafficking Database"), online at http://www-ns.iaea.org/security/itdb.asp; see also Douglas Frantz and Catherine Collins, *The Nuclear Jihadist: The True Story of the Man Who Sold the World's Most Dangerous Secrets...And How We Could Have Stopped Him* (2007).

[2] A non-American company was deliberately selected for this illustration. For good reason, private companies are rarely willing to openly discuss export control violations. The Stimson Center has however, successfully engaged

The Oerlikon Leybold Vacuum incident is revealing and instructive on an additional front. Although company representatives noted that the firm always "actively support[ed] the goal of nonproliferation," its motivation to be a proactive partner in nonproliferation came only *after* the discovery of its vacuum pump technology in Iraq. The incident thus exposed major proliferation risks and dealt a serious blow to the company's image and bottom line. Soon thereafter, an internal "Leybold Charter" was adopted that called for stringent, voluntary self-restraint in export matters and that explicitly expressed support for nonproliferation goals.

Regrettably, the Oerlikon incident is not an aberration. Governments around the world, led most often by the United States—one of the most rigorously regulated and enforced marketplaces on the planet—continuously struggle to keep up with rapidly changing technology by developing new restrictions and regulations backed by an array of export control standards and the threat of fines and prosecution. Nonetheless, we continue to see incidents of illicit or otherwise undesirable technology diffusion, including from the United States.[3]

The Need for a "New Normal" in Public-Private Relationships

The rudderless, fragmentary state of public-private cooperation on national security issues is a strategic weakness for the United States. The threat environment continues to evolve at great speed. Equally important—but less appreciated by many in the national security community—is that the nature of governance itself is changing just as rapidly. These two trends are highly related, and the US government (USG) will need to confront the latter if it is to have any hope of adapting successfully to the former.

What we colloquially reduce to the term "global supply chain" is actually a complex, multi-layered system of assets owned primarily by private sector entities. Industry uses these assets to conduct cross-border transactions in the air, sea, land, space, and cyber domains, which collectively can be thought of as a commons or a public good that is shared across national boundaries. The central challenge for proliferation prevention within the supply chain—whether the front end with the suppliers of raw materials to technology innovators, the back end with end users, or at intervening points—is twofold:

- **Jurisdiction.** In the main, the authorities of national governments are limited to national borders. Bilateral, multilateral, and international initiatives go some way toward filling the vacuum beyond, but they employ the same types of mechanisms seen at the state level—often, less effectively.
- **Complexity and speed of change**. The efficiencies of global commerce and the ever-expanding horizons of new technologies demonstrate how outmoded many traditional legal, regulatory, and bureaucratic concepts have become.

These dual asymmetries open new pathways and new incentive structures for trafficking in dual-use materials and technologies that could support a chemical, biological, radiological, or nuclear (CBRN) capability. By exploiting legitimate commercial and financial services, these illicit procurement networks often hide in plain sight. The same insidious infiltration of legitimate trade has been seen with other forms of transnational crime, including trafficking in counterfeit goods, narcotics, and humans. The relationship

---

in a public dialogue with major blue chip firms in the United States on best business practices for preventing illicit diversions of technology. See, e.g., Kevin Cuddy (Export Controls Manager, General Electric), "Compliance with Targeted Sanctions: Watchlist Screening," (Stimson, 2011), online at http://www.stimson.org/compliance-with-targeted-sanctions-watchlist-screening/

[3] See, e.g., the Department of Justice's running update of major violations: "Summary of Major US Export Enforcement, Economic Espionage, Trade Secret, and Embargo-Related Criminal Cases" (February 2013). Accessed online at: http://www.justice.gov/nsd/docs/export-case-fact-sheet.pdf

among these different illicit activities bears directly on the nonproliferation research agenda, meriting further comment below. Whatever the extent of that relationship, the toll of illicit trafficking on public and private interests alike is significant.

To be clear, traditional law and regulation are, and will remain, the central organizing principles for maintaining order and, more to the point, for proliferation prevention. But it would be far more preferable to leverage the market itself to reinforce sound regulations and more systemically discourage or impede these illicit activities much earlier. Put differently, if the market presented superior options to the various actors throughout global economic networks who, knowingly or otherwise, facilitate illicit trade, it would benefit both the public security interest and legitimate commerce.

Calls for improved public-private cooperation on these issues have grown louder in recent years. And there are many to whom we owe a debt for advancing the dialogue as far as it has come. Unfortunately, most ensuing efforts—with some notable exceptions referenced below—have unfolded within the traditional and rigid conceptual framework of how government and industry should relate to one another. Thus, any progress that has been achieved has been promptly rolled back by familiar bureaucratic obstacles. To enable a truly modernized strategy for proliferation prevention, we must change the narrative on public-private mechanisms in two ways:

1. ***We must engage a broader set of industry stakeholders for a more informed view of how security imperatives interact with market dynamics, both across and within sectors.***
2. ***We must explore more aggressively the potential of market-based incentives to meaningfully and sustainably change industry behavior in the service of government's security objectives.***

While this is a crucial new frontier in the public-private conversation, it will not necessarily be easy. It certainly does not offer a silver bullet that will immediately degrade illicit networks or prevent any incident of proliferation. But the prospects of continuing the status quo look much worse.

An Emerging "Threat Convergence"

Even the most cursory review of the state of the world today leaves little doubt that security, stability, and further progress are being challenged by a growing array of vexing security threats that do not respect national borders or policy stovepipes. Prevailing indicators reveal that these problems, often subsumed under the seemingly innocuous heading of "transnational threats," are a growing cancer on the human condition and threaten an increasingly violent future for the planet. For example:

- **One quarter of the annual $4 billion small arms trade is unauthorized or illicit.** Every day around the world, one thousand people die because of guns.[4] And on average, 300,000 intentional firearm deaths occur each year as a direct result of armed conflict.[5]
- **According to the US Government, approximately 800,000 incidents of international human trafficking occur every year.** This figure does not include the millions of others who are trafficked within their own countries. In total, the International Labor Organization (ILO)

[4] The International Action Network on Small Arms, "2006: Bringing the Global Gun Crisis under Control" (2006). Accessed at http://www.iansa.org/members/IANSA-media-briefing-low-res.pdf

[5] Kimberly L. Thachuk (ed.), *Transnational Threats: Smuggling and Trafficking in Arms, Drugs, and Human Life* (2007), p. 65.

estimates that there are 20.9 million people around the world in forced labor, bonded labor, forced child labor, and sexual servitude. Other estimates range up to 27 million individuals.[6]

- **From January 1993 to December 2012, 419 incidents involving unauthorized possession and related criminal activities were confirmed by the IAEA's Illicit Trafficking Database (ITDB).** Sixteen illicit nuclear proliferation incidents reported to the ITDB involved highly-enriched uranium and plutonium.[7] Just five or six kilograms of highly-enriched uranium—about the size of a grapefruit—is sufficient to build a crude terrorist nuclear weapon capable of killing tens of thousands of people with a single attack.

- **The spread of counterfeit goods has become a global phenomenon in recent years, and the range of goods subject to infringement has increased significantly.** According to the study of the Counterfeiting Intelligence Bureau (CIB) of the International Chamber of Commerce, counterfeit goods make up 5 to 7 percent of world trade. The US Federal Bureau of Investigation (FBI) believes that the first bombing of the World Trade Center was financed by the sale of fake Nike and Olympic t-shirts by followers of Sheikh Omar Abdul Rahman.[8]

- **As the international financial industry ballooned through the 1990s, money laundering grew commensurately.** By 1998, the International Monetary Fund (IMF) estimated the global flow of dirty money to be at 2 to 5 percent of the global economy. More recent estimates place the flow of laundered money at upwards of 10 percent of global gross domestic product (GDP).[9]

- **And according to the UN Office on Drugs and Crime, the global drug trade is worth an estimated $322 billion annually with 52,356 metric tons of opium, cannabis, cocaine, and amphetamine-type stimulant (ATS) produced each year.[10]** The economic costs alone of drug abuse in the United States have been estimated at $193 billion per year.[11] And, an estimated 0.6 percent of the planet's adult population—about 26 million people—are considered to be problem drug-users.[12]

Although each of these transnational threats is a costly tragedy in its own right, the aggregate consequences reach much further. Criminal networks invade weak and failing states, capturing key government agencies, undermining and ultimately controlling many of the critical functions of government—customs and border controls, the judicial system, police, and banks. Moreover, these

---

[6] US Department of State. "Trafficking in Persons Report" (June 2012). Accessed at http://www.state.gov/documents/organization/192587.pdf

[7] International Atomic Energy Agency. *Illicit Trafficking Database*. Accessed at http://www-ns.iaea.org/security/itdb.asp

[8] ICC Counterfeiting Intelligence Bureau, *Countering Counterfeiting: A Guide to Protecting and Enforcing Intellectual Property Rights* (1997); United Kingdom and Organization for Economic Co-operation and Development, "The Economic Impact of Counterfeiting and Piracy: Executive Summary" (2007), accessed at http://www.oecd.org/dataoecd/13/12/38707619.pdf

[9] Moises Naim, *Illicit: How Smugglers, Traffickers, and Copycats are Hijacking the Global Economy* (New York: 2006), p.16.

[10] United Nations Office on Drugs and Crime, "2008 World Drug Report" (2008). Accessed at http://www.unodc.org/documents/wdr/WDR_2008/WDR_2008_eng_web.pdf

[11] Senator Jim Webb, "Opening Statement," Presented to the Joint Economic Committee hearing on "Illegal Drugs: Economic Impact, Societal Costs, Policy Responses," Washington, DC (June 19, 2008). Accessed at http://jec.senate.gov/index.cfm?FuseAction=Files.View&FileStore_id=2bdd4434-1328-44ad-9940-6f052936b3f5

[12] National Drug Intelligence Center, US Department of Justice, "The Economic Impact of Illicit Drug Use on American Society" (April 2011), p. ix. Online at: http://www.justice.gov/archive/ndic/pubs44/44731/44731p.pdf

networks increasingly leverage each other and even converge, with crime groups profiting from not just one but various trafficking and smuggling activities, the same routes or means of facilitation being used for these activities, and transnational organized crime's growing links to terrorism.[13] One of the most worrisome consequences of this combined threat is the fear that these networks could facilitate the trafficking of WMDs, WMD materials, and other dangerous weapons and technologies that threaten global security.[14]

For instance, according to the US Drug Enforcement Agency, terrorist "enablers" in the Tri-Border Area of South America funnel the profits of their drug enterprises through money laundering operations to Islamic Jihad and Hezbollah.[15] And the black market nuclear network of A Q Khan, preying in part upon legitimate technology manufacturers and shipping companies in a dozen countries around the world, helped facilitate the nuclear programs of North Korea, Iran, and Libya, and may have even had interactions with Al Qaeda.[16]

If these cases offer a lesson that should be learned, it is that the complexities of today's transnational trafficking threats are interconnected, and cannot be solved within the traditional policy stovepipes and state-centric thinking that have dominated policymaking in the past. Although large portions of narcotics, counterfeit goods, or illicit financial flows occur outside of legitimate industry—on the backs of mules across the Afghan border, or aboard pleasure craft from the Caribbean into the American homeland—the sheer volume of these flows suggests that the lion's share intersect at some point with the legitimate supply chain. While governments have worked hard to educate, regulate, and enforce standards of good behavior across these industries, the inexorable growth of illicit trafficking in all manner of contraband indicates that these efforts have led to the displacement, rather than amelioration, of the threat.

For over forty years, technology denial regimes reflected the fault lines of the world's ideological and structural conflicts.[17] The spread of weapons technology, for instance, has been held in check by a patchwork of denial regimes at the international and state level. Accordingly, the major nonproliferation treaties—the Treaty on the Non-Proliferation of Nuclear Weapons (NPT), the Biological Weapons Convention (BWC), and the Chemical Weapons Convention (CWC), as well as most international conventions and protocols against trafficking and organized crime—the Convention against Transnational Organized Crime, the Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children, the Protocol against the Smuggling of Migrants by Land, Sea and Air, or the Protocol against the Illicit Manufacturing and Trafficking in Firearms—reflect state-centric solutions to the proliferation challenge, meaning that the state is assumed to be the main repository of the item being controlled and the guarantor of its security from illegitimate entities. However, none of these treaties or conventions themselves encompasses specific measures related to non-state actors (private industry) as a potential source of illicit trade and proliferation.

---

[13] John Rollins and Liana Sun Wyler, "Terrorism and Transnational Crime: Foreign Policy Issues for Congress," Congressional Research Service report for Congress (October 19, 2012). Accessed online at: http://www.fas.org/sgp/crs/terror/R41004.pdf

[14] David M. Luna, Session I on Threat Convergence at the Trans-Atlantic Symposium on Dismantling Transnational Illicit Networks, remarks as prepared (May 17, 2011). Accessed at http://www.state.gov/j/inl/rls/rm/164306.htm.

[15] Anthony P. Placido, statement before the House Committee on Oversight and Government Reform, Subcommittee on National Security and Foreign Affairs, hearing entitled "Transnational Drug Enterprises (Part II): Threats to Global Stability and U.S. Policy Responses" (March 3, 2010). Accessed at http://www.justice.gov/dea/pr/speeches-testimony/2012-2009/ct030310.pdf.

[16] Brian Michael Jenkins, *Will Terrorists Go Nuclear?* (2008).

[17] "Structural conflict" was coined by Stephen Krasner in his book *Structural Conflict: The Third World Against Global Liberalism* (1985), which discusses the North-South divide extensively, including the formation of the Group of 77 and the subsequent calls for a New International Economic Order.

Meanwhile, globalization has yielded a competitive landscape whereby the most vigilant private firms face economic disincentives to proactively combat illicit activity absent a direct and deleterious impact on profit. In the eyes of many private actors—particularly in the dual-use technology and shipping sectors—government regulation has often been haphazard and inimical to fair competition. As a result, relations between government and industry have eroded appreciably over the past two decades and, along with it, much of the rationale for industry to exceed legal obligations in the prevention of illicit activity that does not immediately impinge upon its own business operations.[18]

With 95 percent of the world's consumer base living outside of the United States, and with uneven regulation across virtually all 196 countries on the planet, companies and business associations consistently call for a level playing field in order to ensure fair competition—or, at a minimum, countervailing incentives to accept uneven regulatory standards.[19] Even companies prepared to act above the letter of the law can find their operations compromised by nefarious actors exploiting legal loopholes and weak links in the supply chain for their own ends—and at great expense to international security.

In sum, this growing disparity in regulation, combined with an increasingly outdated denial toolkit on the part of governments, has fomented a set of dynamics that further confound the ability of regulatory regimes to adequately address trafficking challenges. Within the context of globalization, the rise of non-state actors—including terrorist groups, non-governmental organizations and multinational corporations, the pace of technological advances, increasing trade, transport and communications, and financial liberalization provide a confluence of factors that increasingly diminish the ability of the state or multilateral organizations to provide effective solutions.[20] As such, there is growing recognition that success requires a layered defense involving efforts to inculcate rigorous industry involvement. A growing litany of government, business, and academic reports has concluded that if government fails to engage industry as the first line of defense in the detection and disruption of illicit networks, it is less likely to achieve enduring and cost-effective solutions to the array of trafficking challenges.[21]

---

[18] Finlay interviews (2008-2011).

[19] See e.g., the Customs-Trade Partnership Against Terrorism (C-TPAT), which offers benefits and incentives to private sector companies that meet or exceed C-TPAT supply chain security criteria and best practices. See also: Business Roundtable, "Roadmap for Growth," 2011, accessed online at: http://businessroundtable.org/uploads/studies-reports/downloads/Roadmap_for_Growth_Full_Report_1.pdf; and US Chamber of Commerce, "Global Regulatory Cooperation Project," accessed online at: http://www.uschamber.com/grc

[20] See, e.g., Moises Naím, *Illicit*; David Albright, *Peddling Peril: How the Secret Nuclear Trade Arms America's Enemies* (2010); Michael Kenney, *From Pablo to Osama: Trafficking and Terrorist Networks, Government Bureaucracies, and Competitive Adaptation* (2007); Holmes (ed.), *Terrorism, Organised Crime and Corruption: Networks and Linkages* (2007); Willem van Schendel and Itty Abraham, (eds.), *Illicit Flows And Criminal Things: States, Borders, And the Other Side of Globalization* (2005); Richard Friman and Peter Andreas (eds.), *The Illicit Global Economy and State Power* (1999); Catherine Collins and Douglas Frantz, *Fallout: The True Story of the CIA's Secret War on Nuclear Trafficking* (2011).

[21] Gretchen Hund and Amy Seward, "Self-Regulation to Promote Nonproliferation," *Public Interest Report* (Federation of American Scientists, Spring 2011); Ian J. Stewart, "The Anti-Proliferation Hub," accessed online at: http://www.antiproliferation.com/; USAID, "USAID Anti-trafficking in Persons Programs in Asia: A Synthesis" (November 2009), accessed online at: http://www.usaid.gov/our_work/cross-cutting_programs/wid/pubs/Asia_Synthesis_Anti_Trafficking_508.pdf; US Chamber of Commerce, "U.S. Chamber Applauds Public-Private Partnership in Defeating Counterfeiting Ring," July 24, 2007, accessed online at: http://www.uschamber.com/press/releases/2007/july/us-chamber-applauds-public-private-partnership-defeating-counterfeiting-rin

Objective

This report seeks to open a new dialogue on how to address each of these challenges: the evolving proliferation threat, the growing imperative to engage industry, and the convergence of transnational security challenges. Furthermore, the study seeks to fill gaps in the existing literature by soliciting the perspective of private industry. Whereas the prevailing approach to proliferation prevention consistently begins with a definition of threat by governments, and invariably leads to designated solutions by that same constituency, this study seeks first to solicit the input of private industry in order to delineate a series of recommendations on how to initiate broader dialogue between business and government on roles and responsibilities, and to ultimately stem proliferation and related transnational trafficking activities. The solutions proffered below aim to identify meaningful mechanisms to incent both profitable and secure market behavior on the part of industry.

Methodology

This research initiative initially engaged the private sector in a series of discussions designed to delineate mechanisms that might yield the sharing of critical information and the development of practical, scalable self-regulatory activities that do not unreasonably interfere with business operations, and both of which would contribute meaningfully to global counter-trafficking and proliferation prevention. By better sharing information on illicit inquiries, procurement and other trafficking networks can be more readily identified and shut down by government. By establishing models of self-regulation that complement existing government standards, and that are enforced by self-interest, more enduring buy-in across industry will yield transactional standards that are less favorable for illicit trade in all manner of contraband. Unlike previous efforts to educate or enforce regulatory standards that are considered antithetical to business interests, Stimson has worked with industry to develop ideas for positive inducements for heightened compliance and information sharing.

These measures will not be a panacea to transnational criminal activity, but instead will enable a complementary, layered approach to prevent trafficking and proliferation. As such, the project focused on four illustrative industry sectors: **dual-use technology manufacturers, the radiopharmaceutical sector, the shipping/transport sector, and the insurance industry**. These four sectors of course do not capture all global economic activity. They can, however, help build a template for a more comprehensive approach to industry that government and industry, working together, can adapt to the applicable market and security variables. A description of the project rationale for selecting each of these industries, along with a brief overview of top-line findings, is below.

Dual-use technology innovators and manufacturers

The dual-use technology sector was selected as a result of an initial summary analysis of the degree of persistent regulation from national security agencies. This sector, and particularly the part that relates to the proliferation of nuclear weapons, has been the focus of US government regulators since the dawn of the nuclear age.

Dual-Use Technology Manufacturers: Principal Critiques of Regulatory Environment*

- Belief by some in USG that government can act as its own industrial and technological systems integrator—in fact, that role requires deep systems engineering expertise
- Need "trusted exporter" regimes
- Insufficient USG guidance on anticipated program/tech requirements
- Limited pool of highly skilled labor—need education/immigration changes
- "Information sharing" with USG largely a one-way relationship

**Author interviews*

Furthermore, on several occasions, these dual-use technology innovators and manufacturers told Stimson that US regulators have asked industry to sacrifice potentially legitimate sales in the interest of national security.[22] These regulations have been backed by an array of export control standards and the threat of fines and prosecution. Yet despite these efforts, incidents of technology diffusion even from the United States—perhaps the most rigorous regulated and enforced market—continue.[23]

Incidents such as that described above involving Oerlikon Leybold surface with increasing frequency and suggest a growing challenge to the existing regimes, as well as the decreasing wherewithal of governments alone to implement effective solutions.[24] Unfortunately, to date the nonproliferation community has not focused sufficient attention on quantifying the scope of the challenge and identifying industry's potential role in developing workable solutions that go beyond more intrusive state enforcement. According to some of Stimson's industry participants, and to Oerlikon itself, the troubled state of government/industry relations in the United States has set back progress in establishing effective public-private partnerships even further than the lag seen in Europe.

Shipping industry

If there is a common sector that touches upon virtually every flow of contraband—be it WMD proliferation, narcotics, counterfeit intellectual property, or small arms and light weapons—it is the legitimate shipping industry. Developing a more self-aware, more active, and more positively incented shipping sector cannot but promote global counter-trafficking efforts.

Today, innovative transportation technologies have accelerated the transshipment of goods around the globe. Containerization, larger and more efficient ships, roll-on/roll-off cargo container vessels, new loading and unloading tools, more efficient port management, improved logistics, and satellite navigation and tracking have all become part of a critical circulatory system within which globalization itself has been able to flourish. By 2007, the volume of international seaborne trade reached an unprecedented eight

[22] Finlay interviews (2008-2011).

[23] Even a cursory survey of the Department of Commerce's annual reports to Congress indicates a steady number of criminal cases criminal resulting from export control violations: 2001: 27 (23 against corporations); 2005: 31 (10 against corporations), 2010: 71 (41 against corporations), see: Bureau of Industry and Security Annual Report for Fiscal Year 2002, U.S Department of Commerce Bureau of Industry and Security, 2002, pp. 57-62 <http://www.bis.doc.gov/news/2003/annualreport/appendixd_p.pdf>; (2) Bureau of Industry and Security Annual Report for Fiscal Year 2005, U.S Department of Commerce Bureau of Industry and Security, 2005, pp. 37-40 < http://www.bis.doc.gov/news/2006/annualreport/bis_annualreportcomplete05.pdf>; and Annual Report to the Congress for Fiscal Year 2002, U.S. Department of Commerce Bureau of Industry and Security, 2010, pp. 25-40 < http://www.bis.doc.gov/news/2011/bis_annual_report_2010.pdf>. Also see: Department of Justice, Summary of Major US Export Enforcement and Embargo-related Criminal Prosecutions: 2007 to the Present, September 2011, accessed online at: http://www.justice.gov/nsd/docs/summary-eaca.pdf

[24] Eric Lipton, "US Alarmed as Export Veer Off Course," *New York Times* (April 2, 2008), p. 1.

billion tons. Even in the midst of a global economic slowdown, at any given moment, there are some 20 million intermodal freight transport containers moving around the globe. More than 4,600 ships carry many of those containers on over 200 million trips per year.[27]

Shipping/Transportation Firms: Principal Critiques of Regulatory Environment*

- USG-designed incentives (as in C-TPAT) often are not meaningful/relevant or do not materialize as promised
- "Information sharing" with USG largely a one-way relationship
- Insufficient understanding by USG of many different business models across supply chain and transport space

**Author interviews*

However, as the global flow of legitimate goods has grown, so has the transshipment of illicit items—small arms, drugs, counterfeit products, and perhaps most worryingly, weapons-useable materials and technologies. In response, governments have introduced an array of rigorous security measures to help weed out contraband from the legitimate supply chain: the Customs-Trade Partnership Against Terrorism (C-TPAT), the Container Security Initiative, new air cargo security rules, the Trade Act of 2004 (including the 24-hour rule), the World Customs Organization Framework, the SAFE Ports Act, and the Authorized Economic Operators (AEO) guidelines are just a few.

As with the dual-use technology sector, these additional regulations layered in the wake of the 9/11 terrorist attack have created similar push-back and criticisms from industry, rather than meaningful partnerships with mutual benefit. For instance, four years after 9/11, the Bureau of Customs and Border Protection (CBP) inspected less than three percent of the 20 million inbound shipments to the United States annually. Unable to effectively police the supply chain, CBP introduced the C-TPAT, which mandates that US companies help shoulder the burden of cargo screening. While a reasonable premise, companies canvassed by this study routinely complained that participation in the C-TPAT—today a near necessity for all major companies in the sector—offers few meaningful incentives. Further investigation reveals that those incentives were defined not by industry, but by government regulators and, as such, have in many cases failed to meet the minimal standards to provide meaningful benefit to industry.[28]

Properly incenting the shipping industry—in addition to sound regulation—would better enlist the long-term support of legitimate supply chain companies and help counter the illicit flow of items around the globe. Identifying ways to transform the industry from a conveyor belt into a "choke point" for these illicit items without hampering the competitiveness of legitimate companies will be critical for proliferation prevention and other counter-trafficking efforts.

---

[27] James S. Cannon, "Container Ports and Air Pollution: An Energy Futures, Inc. Study," (Energy Futures Inc.: 2009), accessed online at: http://www.mvo.nl/Portals/0/duurzaamheid/biobrandstoffen/nieuws/2009/05/2009PortStudy.pdf

[28] The motivations of private industry are often misunderstood by those outside of discrete sectors. By way of example, US regulatory authorities and academics have long assumed that the growth of piracy off the Horn of Africa yields a significant detrimental effect on global shipping interests. While large shipping firms like Maersk recognize that piracy has raised costs, for most major firms, these costs are viewed as eminently manageable. Industry estimates the "cost" of piracy at $12 billion per year. While this may seem significant, across a $12 trillion dollar industry, piracy is viewed as a modest tax on the global economy. Accordingly, the global shipping industry is not as concerned about terrorism or piracy than it is about insufficient physical port infrastructures around the world, corruption and ungoverned spaces in foreign countries, or pilferage. Interviews on October 26, 2011 (Brian Finlay, interviewer); see also: Lara L. Sowinski,"Are DHS Security Initiatives Living Up To Their Promises?," World Trade WT100, January 1, 2005; and Barry Brandman, "Security Brief: It May not be Perfect, but C-TPAT's here to stay," DC Velocity, November 2005, pp. 35-38.

Radiopharmaceuticals

At present, more than 10,000 hospitals worldwide actively use radioisotopes to detect and treat diseases. Radiopharmaceutical research involves radioisotopes attached to drugs administered to patients for more than 50 different types of diagnostic tests. And in the US alone, there are some 18 million nuclear medicine procedures per year among 305 million people.[29]

Radiopharmaceutical Manufacturers: Principal Critiques of Regulatory Environment*

- Uneven regulatory treatment of certain imaging technologies
- Little desire within USG for nuclear-science technology transfer to industry, even though it would be "win-win"

**Author interviews*

The bulk of radioisotopes used, like technetium-99, are derived from highly enriched uranium (HEU) and the nonproliferation community has rightly raised concerns about the lack of regulation at both ends of this industry's spectrum—from the major producers of medical isotopes to the sites that secure the material.[30] Regulators are also now starting to consider another critical component in the radiological supply chain as new technologies are introduced: the actors between the industry and end-users, the diagnostic machine fabricators who represent the critical hub in the research, development, and manufacturing sector.

In this space, some in the nonproliferation community have advocated for the conversion of these facilities from HEU to low-enriched uranium (LEU) production.[31] Elected officials and NGOs have also pointed to the ease with which highly dispersible material, such as Cesium 137, could be removed from inadequately secured sites and the possibility of non-state actor use of a radiological dispersion device. Most point to hospitals and other treatment centers, but radiological sources are used also in the construction, petroleum, and airline industries. In response, the Department of Energy's Global Threat Reduction Initiative launched a voluntary program to secure this material.

Insurance industry

The insurance industry is an essential partner to each of the above sectors. As such, its influence and leverage over the proliferation and counter-trafficking space cannot be underestimated. Insurance delivers essential services to the market that simultaneously could be leveraged and expanded to address global security challenges: risk sharing, price discovery, and, importantly for national security, the identification of risk mitigation measures. While risk sharing and price discovery are attributes of every functioning insurance marketplace, industry—both the insurers and the insured—can help identify measures that would mitigate risks, reduce insurance costs, and extend coverage. The market itself can be leveraged to develop new standards and to incentivize positive adherence to existing or new standards of self-regulation, as defined by these discrete industry sectors.

---

[29] World Nuclear Association, "Radioisotopes in Medicine," October 2001, accessed online at: http://www.world-nuclear.org/info/inf55.html

[30] Today, there are five major producers of medical isotopes: MDS Nordion (Canada), TycoHealthcare/Mallinckrodt (The Netherlands), Institut National des Radioéléments (Belgium), NECSA/NTP (South Africa), and Covidien (Ireland); together, they provide more than 95% of the global supply of medical isotopes.

[31] Cristina Hansel, "Nuclear Medicine's Double Hazard: Imperiled Treatment and the Risk of Terrorism," in *Nonproliferation Review*, Vol. 15, No. 2, July 2008, pp. 185-208.

Insurance Firms:
Principal Critiques of Regulatory Environment*

- Systemic bias for mislabeled cargo
- State-based regulatory regime means industry does not share in many benefits that adjacent industries enjoy
- USG does not understand how insurance industry works, or how products could advance USG goals in some circumstances

**Author interviews*

For industry, compliance with best-practice standards is voluntary but could be incentivized through multiple factors—including through insurance, thereby building a business case for heightened self-regulation. With standards, the insurance industry will benefit from better risk information, and potential claims will fall as compliance with standards increases. In addition, new types of coverage could be incentivized, including perhaps government-based incentives for offering nonproliferation or counter-trafficking mitigation in policies. More strategically, as global risks are reduced or mitigated, both the insured and the insurers benefit.

The Key Functions of Insurance: A Primer

Risk-sharing: Risk premiums from many different insured entities are pooled to cover potential losses. As a direct benefit of insurance, those at risk from an event who comply with certain standards could pay a comparatively smaller premium to the insurer or have lower deductibles. When the insurer later uses accumulated funds to reimburse those parties suffering actual losses, both the insured and society benefit. While risk-sharing in itself may not directly reduce the likelihood or losses from a WMD terror event, most economic activities, from redevelopment of the World Trade Center site in New York, to the reconstruction of the Mumbai hotels destroyed in the recent terrorist strikes in that city, could not happen without it. Insurers have guaranteed that private development can continue in the face of a rising WMD threat.

Price discovery: Price discovery involves assessments of the probability of an insured incident and its frequency and consequences. Insurers rely largely on computer models to help estimate these and insurers' potential payouts. While predicting the likelihood of catastrophic events is challenging, for illicit activities such as theft or diversion, the actuarial science perfected by the insurance industry combined with computer-based simulations and modeling techniques offer a major benefit to insured clients and potentially even to governments seeking to prevent a range of illicit activities that can be modeled. However, given the limited loss history in terrorism- and WMD-related events, insurance pricing is difficult, and typically has relied on federal backstopping when it has been available.

Mitigation: By establishing insurance pricing and cover, the insurance industry mitigates undesirable behavior. This is the process by which insured parties take actions to reduce their expected losses in order to obtain lower premiums, lower deductibles and qualify for coverage. For example, one incentive to mitigate is created by risk-based premiums, whereby each insured party pays a premium commensurate with individual risk.

* * *

Representatives of these four industry sectors contributed input to this report. In all, the project team conducted approximately 52 interviews with USG representatives and 85 interviews with industry stakeholders between June 2012 and March 2013. US government interlocutors spanned eight executive departments, the National Security Staff, and several congressional committees. Meetings were convened in Washington, Boston, New York City, and Miami. For most discussions, interviewers agreed that solicited comments were not-for-attribution. In select cases, Stimson agreed to use industry comments on background only.

Information supporting the findings of this study was drawn largely through the pursuit of answers to the following research questions:

- **What are the specific proliferation or trafficking challenges that might be facilitated by each industry sector?** Before any reasonable effort can be made to address the threat of transnational criminal trafficking of any sort, a comprehensive catalogue must be developed outlining the US Government's understanding of the threat and specific concerns with the industry. What do existing violations tell us about criminal interest in exploiting private industry? What do trends tell us about the evolution of these threats? And what are the future threats that will come to define illicit trafficking patterns that industry should be aware of?
- **What is industry's understanding of the global trafficking challenge?** Government regulations are defined by national security objectives. As tactical implementers, the private sector has a unique perspective on the threat posed and methods used by illicit procurement networks and other transnational criminal agents. How does industry's understanding of the proliferation or trafficking threat differ from the strategic perspective of government and how can we better align these threat perceptions to the benefit of US national security?
- **What are the principal issues of concern for industry with existing regulatory regimes?** Individual corporations and their business associations have long rallied against perceived unfair or unreasonable regulations, whether they are related to export controls, transshipment controls, market approvals or other restrictive government policies. Within each of the discrete industry sectors, what are the key impediments embedded within US law and enforcement practices to creating an internationally competitive playing field? This discussion will then lead into a more fruitful dialogue regarding how some of these outmoded regulations might be supplanted by industry self-regulation, thereby creating an immediate incentive for industry inculcation of these standards.
- **What programs has industry initiated already to limit the possibility of proliferation?** For those companies that have either reached a level of growth or sophistication in which their brands may suffer from the public relations implications of an illegal transfer, or those that have been the target of legal sanction in the past, sophisticated mechanisms of self-regulation have often been instituted. What are these best practices within each of the four industrial sectors, and what can others learn from these internal practices?
- **What more could each industry sector do to prevent illicit trafficking?** Instinctively, all companies and business associations will push back against the need for enhanced regulation. Yet virtually all companies also recognize that there are additional measures that *could* take place to enhance national security. The closed door working groups will solicit feasible self-regulatory standards that will both disrupt illegal activity while not unreasonably interfere with business practices.
- **What are the appropriate incentives that would bring industry to the table and inspire a fundamental buy-in from government regulators**? In the face of the global economic slowdown, and an increasingly unevenly regulated global marketplace, companies cannot afford to engage in non-mandated practices that could threaten their bottom lines. What are the market-based incentives that could encourage broader buy-in from industry to more rigorous self-regulatory practices?

Assumptions

The project proceeded from two principal assumptions:

1. Governments' primary concern in the proliferation context is the prevention of a wider diffusion of materials, technologies and know-how to would-be proliferators at the state or sub-state levels.

Conversely, while well-intentioned private companies are rightly concerned with the proliferation challenge, their actions must also reflect their core obligations to their investors or shareholders. Yet despite these differing motivations, private industry can be brought more meaningfully into nonproliferation and counter-trafficking compliance beyond facile appeals to corporate social responsibility.

2. While positive inducement to altered industry behavior is rightly viewed as an under-exploited driver for enhanced prevention, the authors recognize that legal regulation is and will remain a fundamental necessity. Moreover, we recognize that for some mission areas, and for some functions, private sector cooperation is either more difficult to establish or altogether inappropriate. For instance, the sharing of certain sensitive intelligence with industry interlocutors, or even the engagement of specific companies over others may contravene US national law, and thus is impractical. Ensuring the appropriate balance between punitive regulation and positive incentives is more properly the focus of this study.

Approach

Trafficking in CBRN materials (especially nuclear) was the principal threat motivating the Stimson project. Nonetheless, this effort has sought to be essentially threat-agnostic—more properly, it has adopted a "threat-convergence" perspective. Our belief is that, apart from those engaged in highly technical work, one is most likely to advance the nonproliferation agenda when taking a broader view of how illicit trafficking activities are situated within the complex, interdependent networks that drive the global economy. According to multiple US intelligence sources interviewed by the authors, Western intelligence agencies have devoted much attention since 2001 to identifying connections between the trafficking in WMD items and materials, and the trafficking in other (unrelated) forms of contraband.

When proceeding with the strict parameters of producer and ultimate customer, evidence for these connections is limited. Yet recent incidents of proliferation also indicate that many of the "facilitator" industries—from shipping to insurance to banking—are common to multiple trafficking portfolios. A WMD-crime-terrorism nexus is coming into view for many officials and experts.[32] In short, the same ship carrying a dual-use nuclear item is equally capable of unknowingly carrying narcotics, counterfeit pharmaceuticals, or even human slaves. As such, considered more expansively, various forms of illicit trafficking are likely to share some common attributes, *whether or not those commonalities are known at any point by any of the individuals or organizations involved*. Informed by this approach, Stimson explored how to better align industry incentives and different modalities for government-industry cooperation, without regard to the particular brand of proliferant activity being pursued.

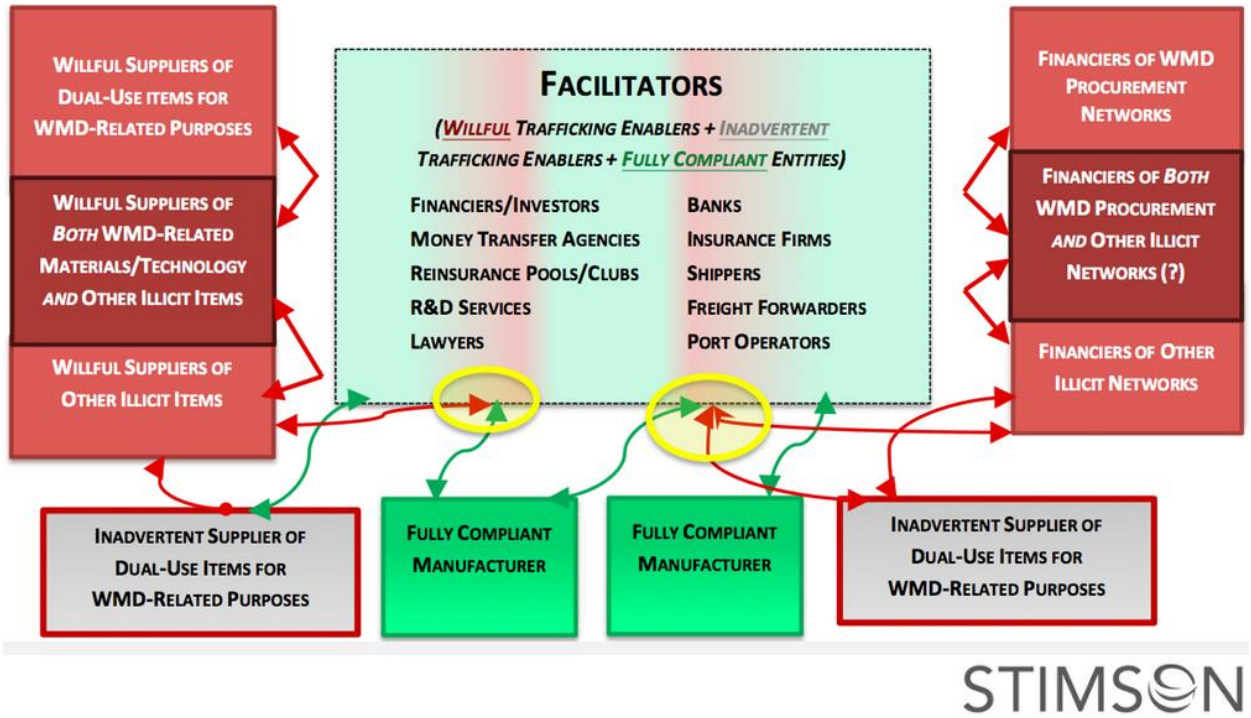
Figure 2 is a stylized representation of the exchange in goods, services, and information that might ultimately support global proliferation networks. It sets the parameters of the challenge beyond the producers of raw materials, technology innovators, and manufacturers, and includes the spectrum of facilitator industries that are critical to supporting the proliferation of CBRN weapons, materials and components, as well as the global movement of licit and illicit goods more generally. The yellow circles mark the key points of interest. They capture network links—that is, the "commonalities" discussed above—between licit and illicit trade. In this case, legitimate firms, as well as deliberate traffickers of

[32] See, e.g., James Clapper, "Worldwide Threat Assessment of the US Intelligence Community," statement delivered to the US Senate Select Committee on Intelligence (March 12, 2013), p. 5, online at http://www.hsdl.org/?view&did=733905; see also George Mason University Terrorism, Transnational Crime and Corruption Center, "Criminal Networks, Smuggling, and Weapons of Mass Destruction," conference report (March 2010), online at https://www.hsdl.org/?view&did=715924.

both WMD materials and other illicit items, interact with some of the same actors from the "facilitators" space. Note that Figure 2 does not make any spatial representations, so the network linkage does not imply a synchronous or asynchronous overlap in physical location.

FIGURE 2

Links Between WMD Procurement and Other Illicit Networks: The "Facilitators" of Terrorism and Transnational Crime



A particular virtue of the threat-convergence perspective is that it can lead stovepiped institutions to build capacity for sharing and adapting information and lessons learned. Security bodies at the national and international levels are increasingly drawing on this approach. Consider the views of this senior practitioner, recorded in a June 2010 study:

> "The IAEA has amassed over fifty years of experience implementing… what was referred to by one senior IAEA official… as a 'vertical approach' to nuclear security aimed at securing radiological and nuclear materials—and blocking their illicit transfer—up and down domestic supply lines and decision-making chains within participating states. When the IAEA's vertical approach is linked to a horizontal approach embracing the programs of other anti-trafficking organizations, nuclear safety and security would be… advanced still further."[33]

But what would enhance this IAEA official's concept—what would position these newly linked anti-trafficking organizations to add the other critical set of tools for the threat-convergence toolkit—is an explicit strategy to leverage private sector resources and expertise. Formulating that strategy first requires an understanding of the challenges that must be navigated.

---

[33] Institute for Foreign Policy Analysis, "A Comprehensive Approach to Combating Illicit Trafficking" (June 2010), pp. 17-8.

Challenges: Interrelated Government-Industry Gaps in Knowledge, Communication, and Structure

The simple desire to improve mission performance by enhancing public-private coordination is but one small step on the road to success. Stimson reviewed a wide body of writing on this topic and incorporated relevant feedback from its own discussions with industry and government. In trying to distill the most common and the most problematic challenges to coordination, three basic themes emerged: government-industry gaps in knowledge, in coordination, and in structural variables. It is important to emphasize that these themes are highly interrelated, with fluid boundaries separating them. The project team still found them helpful to conceptualize independently, both for general understanding and for evaluating potential solutions.

Knowledge Gaps

Establishing a "CONOPS"

Even when they work in related fields or on shared problems, government and industry frequently remain ignorant of what the other party wants, needs, or is empowered to do. Many times, this missing information takes the form of straightforward facts. Even though such a simple knowledge gap could quickly be remedied, it sometimes persists due to related communication problems, such as unease about sharing certain kinds of information. Whatever the cause, if these gaps do not surface early in the process, they can lead to bad assumptions or unexplored opportunities.

Subject matter expertise

In other cases, the knowledge gap centers on more technical information or subject matter expertise. On the whole, industry's profit motive drives innovation so rapidly that government—particularly in an open, capitalist system like the US—has great difficulty keeping pace "at scale." In other words, government is often unable to hire and retain a sufficient number of SMEs for tracking industrial and technological trends, and for supporting associated private sector outreach. There is a similar problem in areas where government chooses to execute research and development (R&D) directly, in support of mission requirements. In a time of intense budgetary pressures, these problems are certain to become more severe—though they might also prompt more innovative mechanisms. The CBRN context is perhaps one of the leading examples in this regard. A September 2012 report by a National Research Council panel recommended that the Department of Defense (DoD) consider shifting some of its CBRN technical research to the private sector, as the number of potential threat vectors continues to climb. Of particular interest, though, the report also encouraged a "tech watch" capability that would give relevant DoD offices "mechanisms for searching and identifying relevant breakthroughs in the literature and private sector."[34]

Stimson's industry and government interlocutors noted several specific knowledge gaps with greater frequency. Of these, we found two to be most pertinent to future public-private coordination on counter-trafficking issues:

[34] National Research Council, Committee on Determining Core Capabilities in Chemical and Biological Defense Research and Investment, *Determining Core Capabilities in Chemical and Biological Defense Science and Technology* (2012), p. 64.

1. ***Within industry, companies in many sectors—not least in the shipping and transport space—need to develop greater sensitivity to how illicit trafficking networks operate.*** A basic example is the need to better track "red flag" information (e.g., various control lists published by government agencies, such as the Commerce Control List [CCL], specifying restricted dual-use items). The export control reform effort is highly likely to increase some of these problems in the short term. Many manufacturers of products currently listed on the U.S. Munitions List will soon face a completely different set of compliance requirements, as some of these products are being migrated to the CCL. Small- and medium-sized businesses, in particular, are likely to need assistance in understanding the rule changes and developing compliant processes.

2. ***Within government, the lack of knowledge of the insurance/reinsurance space is especially acute.*** Stimson heard this concern from sources within government, industry, and other think tanks and academic institutions. In some cases, even those government offices working frequently with the financial services and insurance industries had deficiencies in this regard. We were told of at least one instance in which the problem affected mission performance modestly but directly.

The intra-industry landscape

A longer-term but equally important goal for government is to understand the intra-industry breakdown—the economic and political landscape determining what actors hold what influence. For instance, if a sector has multiple trade associations with at least some overlap, as often happens, which one has the most mindshare? Which standards-setting organizations (whether of a technical, managerial, or other emphasis) seem to shape a particular sector's behavior the most? Occasionally, all of the institutional focal points for such matters can be found within the US. More often, though, these high-level questions of economic and political influence also have an international dimension. The answers do not necessarily turn on market share and revenue streams exclusively. [35] Moreover, these questions might prove sensitive in some contexts—particularly when a government official makes the inquiry—but we found individual companies and trade associations to be open with their evaluations. Seeking input from multiple sources revealed only occasional discrepancies that were rooted more in perspective and opinion than in fact or bad faith.

Communication Gaps

Vocabularies and conceptual frameworks related to risk

Highly specialized communities of interest (COIs) often develop their own terminologies out of necessity, given the technical nature of their work. That issue falls more in the realm of knowledge gaps, discussed above. There is a separate language-related challenge that is subtler but, once identified, somewhat more tractable: differences in how certain terms and concepts are used, adapted, and interpreted. This challenge is rooted less in subject matter expertise than in organizational culture, priorities, and associated processes. And once again, the key issues to consider are not only the government-industry differences, but also the intra-industry and intra-USG differences.

The language and concepts employed to describe *risk*, *risk management*, and *resilience* deserve special attention. Government and industry use these terms regularly when discussing topics like proliferation, supply chains, and international trade. There are many fault lines along which such discussions can be

[35] See, e.g., Tim Büthe and Walter Mattli, *The New Global Rulers: The Privatization of Regulation in the World Economy* (2011).

diverted into other issues or break down into miscommunication and confusion. As a result, several recent and continuing efforts aim to promote shared conceptual frameworks.

For instance, the International Organization for Standardization (ISO) released its ISO 31000 series of standards for risk management processes in 2009, alongside a risk management vocabulary reference.[36] The Department of Homeland Security (DHS) issued its own risk management "doctrine" in April 2011.[37] The World Economic Forum's Risk Response Network has ongoing activities to develop what it calls a "a blueprint for resilient supply chains." Its model deconstructs resilience into four variables: partnerships, policy, strategy, and technology/IT.[38]

In June 2011, the European Commission launched a three-year project called CASSANDRA (Common Assessment and Analysis of Risk in Global Supply Chains), which is promoting use of the so-called Risk Based Audit (RBA) approach among European government agencies. Many government entities base their customs processes and other risk evaluations exclusively on the transaction-level data supplied by the importer/exporter for a particular shipment. In contrast, RBA seeks to incorporate information on underlying process management issues, including a company's internal security policies and standards.[39] Similar principles inform the "account management" concept that DHS's Customs and Border Protection (CBP) has sought to advance; we will briefly consider it in the next section.

Finally, there is much relevant work underway pursuant to the *National Strategy for Global Supply Chain Security* (NSGSCS), released January 2012. One of the implementation tasks, coordinated by DHS's Domestic Nuclear Detection Office and completed in late 2012, was a Radiological/Nuclear Global Supply Chain Risk Assessment. More to the point of harmonizing risk-related concepts, a January 2013 "National Strategy for Global Supply Chain Security Implementation Update" designated the following task as a "priority implementation activity" for 2013: "Develop and institutionalize a process to characterize and assess system-wide risk in coordination with industry and foreign government stakeholders globally."[40] We note other tracks of NSGSCS implementation work below.

Mistrust

Several types of trust-related issues can impede public-private engagements. An underlying issue, of course, is frequently the absence of any extensive relationships or shared cultural norms. For instance, government has an understandable desire to protect sources and methods on intelligence issues, and an understandable need to know what risk a private sector party's international economic activities might pose. Overcoming that type of trust deficit inevitably takes time, but the parties involved can shore up early progress by addressing some of the challenges above—not least, establishing a common operating picture and making explicit how key concepts are to be understood and operationalized. That preliminary work helps ensure that initial expectations and problem definitions are in sync. Otherwise, the parties

---

[36] See ISO, *ISO 31000:2009 Risk management—Principles and guidelines* (2009), online at http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43170; ISO, *ISO Guide 73:2009 Risk management—Vocabulary* (2009), online at http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=44651.

[37] Department of Homeland Security, *Risk Management Fundamentals: Homeland Security Risk Management Doctrine* (April 2011). Online at http://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf.

[38] See, e.g., World Economic Forum and Accenture, "Building Resilience in Supply Chains," (January 2013), p. 21.

[39] http://www.cassandra-project.eu/articles/risk-assessment.html

[40] White House, National Security Staff, "National Strategy for Global Supply Chain Security Implementation Update" (January 2013), pp. 8-9. Online at http://www.whitehouse.gov/sites/default/files/docs/national_strategy_for_global_supply_chain_security_implementation_update_public_version_final2-26-131.pdf.

have a greater tendency to operate at arm's length, foregoing any opportunities to venture outside whatever language might have been agreed upon to guide the relationship (if they were able to reach such an agreement, that is).[41]

Several industry interviewees cited a similar underlying dynamic: Most government security officials have a strong predilection to resort to familiar, traditional tools that "check a box"—that is, that endow these officials with a sense of special insight into, and control over, industry behavior. One such tool of course is the license required for munitions or dual-use items (i.e., items on the US Munitions List or Commerce Control List, respectively). Our industry interlocutors cautioned that officials sometimes become too wedded to particular processes, and too unable or unwilling to consider other ways that security objectives could be achieved—especially if those other ways mean "letting go" in some respect.

A more concrete—and critically important—trust-related challenge can be unwillingness or unease to share sensitive information, *apart* from any legal prohibitions related to classification or similar issues. For both government and industry, there is often fear that information disclosures will have unintended consequences if and when security measures lapse, whether due to human error or deliberate exploitation. Government's concerns on this front relate principally to national security and national economic competitiveness. Private sector concerns tend to focus on brand/reputational risks; liability risks related to, for instance, shareholder claims that a company's participation violates its fiduciary responsibilities; and firm-level or industry-level economic competitiveness. More specifically, the risk to intellectual property can be a stumbling block, particularly when cooperation entails electronic exchange of proprietary information.

Taking a step back, however, one actually sees potential for intellectual property rights (IPR) to be an area of common ground for government and industry in many contexts. As the Office of the National Counterintelligence Executive stated in an October 2011 report to Congress:

> "The migration of most business and technology development activities to cyberspace is making it easier for actors without the resources of a nation-state or a large corporation to become players in economic espionage. Such new actors may act as surrogates or contractors for intelligence services or major companies, or they could conduct espionage against sensitive US economic information and technology in pursuit of their own objectives."[42]

Again, protecting against such exploitation benefits potential US corporate targets, as well as our broader national economic competitiveness. It also is a significant national security issue, as the recent scrutiny of counterfeit electronics in DoD supply chains has shown.[43] This issue, in its own right, could be a point of departure for many innovative public-private efforts at the nexus of IPR and information security. A number of Stimson's industry contacts emphasized some variation on this theme. Recent high-level

---

[41] John Forrer et al., "Public-Private Partnerships and the Public Accountability Question," *Public Administration Review* (May/June 2010), pp. 479-80.

[42] Office of the National Counterintelligence Executive, "Foreign Spies Stealing US Economic Secrets in Cyberspace" (October 2011), p. 10.

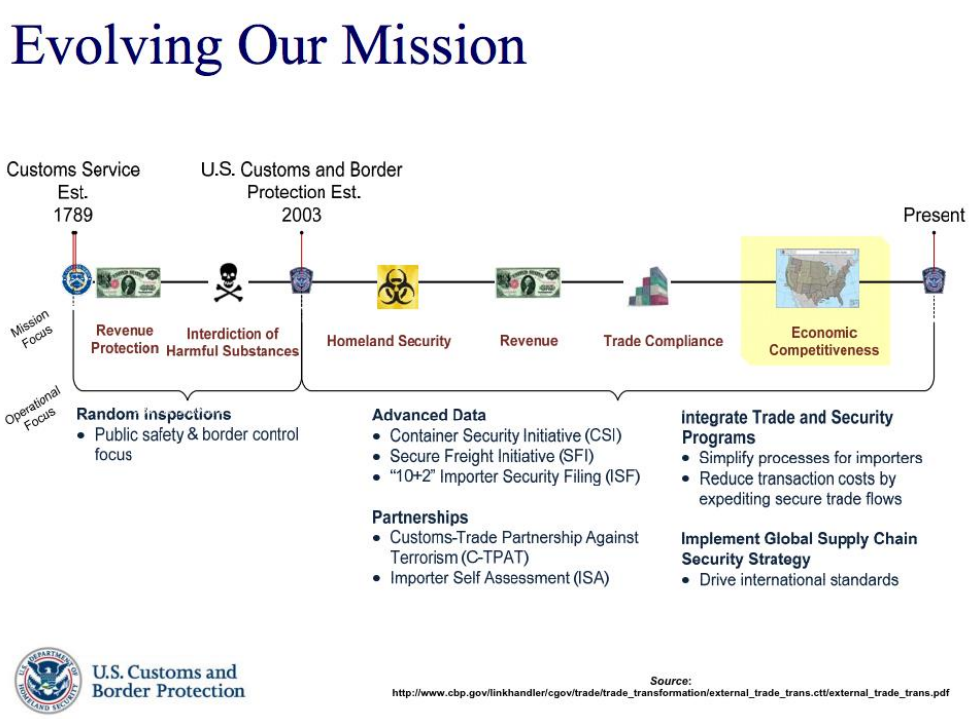
[43] See, e.g., Senate Armed Services Committee, "Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain," S. Rpt. 112-167 (May 21, 2012); see also section 818 of the National Defense Authorization Act for Fiscal Year 2012 (PL 112-81, December 31, 2011), "Detection and Avoidance of Counterfeit Parts"; see also Catherine Ortiz, "DoD Trusted Foundry Program: Ensuring 'Trust' for National Security & Defense Systems," presentation to NDIA Systems Engineering Division meeting (June 20, 2012). Online at http://j.mp/Zcunnd.

policy statements suggest that senior USG officials also are willing to engage with industry in a proactive manner.[44]

Finally, trust can erode when past experience gives one party cause to doubt the other's credibility. Some of CBP's outreach efforts and "trusted trader" programs are instructive in this regard. CBP has adopted industry-friendly language and themes in programs intended to improve supply chain security. As Figure 3 shows, CBP now counts "economic competitiveness" among its mission objectives. This might be what industry wants to hear, and it might indeed be the normative public policy outcome, but it is a major departure for an agency that has two centuries of experience with, and cultural orientation toward, functioning as an enforcer and revenue collector. Problems in making the transition have sometimes been interpreted by industry as an unwillingness to make the transition altogether.

FIGURE 3

The Evolution of CBP's Mission:
Toward "Economic Competitiveness?"



For instance, under C-TPAT, US importers technically are entitled to certain trade facilitation benefits once certified for compliance with specified security standards. CBP claims these benefits include lower probability of border inspections and expedited processing procedures. Stimson's interviews indicate that, for many C-TPAT participants across a variety of sectors, rhetoric and reality have diverged significantly.

Another CBP effort that some industry observers feel has "overpromised and under-delivered" is the "account management" initiative, begun in 1997.[45] Account management refers to evaluating companies

[44] See, e.g., *Administration Strategy on Mitigating the Theft of US Trade Secrets* (February 2013). Online at www.whitehouse.gov//sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

on the basis of historical, company-wide performance on security and compliance issues, rather than on a transactional basis, in which customs officials do not consider factors beyond a given shipment's import/export documentation. In the latter case, companies essentially must start from scratch with every shipment, proving themselves time and again, with a highly compliant company being treated the same as a highly suspect company. When executed correctly, therefore, account management improves security through more sophisticated risk management (risk segmentation) and by providing an incentive for companies whose security practices are sub-standard to make improvements. It also promotes economic competitiveness by facilitating trade.

For most of its history, though, the account management initiative has been short-staffed and otherwise poorly resourced. As of May 2010, CBP estimated that it employed 50 full-time National Account Managers and about 400 part-time Port Account Managers.[46] These personnel serve as primary points of contact for participating companies. The May 2010 figures show a significantly under-resourced effort.

This track record has cost CBP significant credibility with much of industry. But several of Stimson's industry interlocutors who counseled further action to make good on the promise of C-TPAT and account management added an important qualifier: "Action" need not mean "perfection." A good-faith effort to improve identified program deficiencies and to feed industry perspectives into the design of future efforts would be sufficient to maintain industry buy-in for now.[47] And indeed, more recently, there have been some positive developments in account-based management by CBP, including its "co-creation" efforts and the Centers for Excellence and Expertise (CEEs). We will touch on these below.

A final example of counterproductive actions can be seen in several of the Department of Commerce's (DOC) past efforts to modify regulations in order to address some of industry's most consistent objections. The October 2008 proposal to create a license exception for intra-company transfers (ICT) was a particularly disappointing experience for some of our industry interviewees.[48] To simplify, an ICT takes place when one part of a company provides a controlled item or sensitive information to another part of the same company—including, for example, an overseas affiliate—for internal company use. The definition also encompasses providing sensitive information to a foreign national working in the US (a "deemed export"). Under the DOC's Export Administration Regulations, every ICT requires a license.

For many companies, compliance with this mandate is quite time-consuming. Moreover, the firms most affected tend to have the most stringent supply chain security processes and the most repeated transactions, so the license essentially is superfluous. Instead of providing these companies with a better alternative that also would enable DOC licensing officers to focus more time on higher-risk transactions, the 2008 proposal contained a byzantine compliance process of its own. Industry's cost-benefit assessment was that it made more sense to continue the status quo, seeking individual licenses for each transaction.

More recently, the strong and consistent outreach on export control reform (ECR) by Commerce and other departments has impressed many private sector stakeholders. In public and behind closed doors,

---

[45] http://www.cbp.gov/xp/cgov/trade/trade_programs/account_management/

[46] Testimony of Frank Vargo (Vice President of International Economic Affairs, National Association of Manufacturers) before the House Ways and Means Committee, Subcommittee on Trade, on "Customs Trade Facilitation and Enforcement in a Secure Environment" (May 20, 2010). Online at http://www.nam.org/~/media/9091BD4E1CA64EE28AF17FE9345099A7/NAM_Testimony_WMs_Customs.pdf.

[47] Finlay/Olson interviews with shipping and logistics firms (2012).

[48] DOC Bureau of Industry and Security, "Export Administration Regulations: Establishment of License Exception Intra-Company Transfer (ICT)," *Federal Register* vol. 73 no. 193 (October 3, 2008). Online at http://www.gpo.gov/fdsys/pkg/FR-2008-10-03/pdf/E8-23506.pdf.

several industry figures have said that, for the companies affected, the public-private dynamic is at one of its strongest points in recent memory. Much works remains for the larger ECR effort, but on that front and others, there seems to be a strong foundation for further progress.

The fact that CBP and Commerce both have made inroads in areas where they stumbled not long ago is testament to the importance of patience and persistence on the part of all involved in public-private initiatives. Yet in a competitive, profit-driven climate, industry is not usually best suited to patience. Thus the earlier struggles at CBP and Commerce also are an argument for government and industry to risk-manage their own process, as it were. Put differently, spending some additional time on the front end to identify more than one shared objective in the relevant problem space keeps some doors open even when another closes. In like manner, exploring more than one modality—say, one highly formal mechanism with multiple parties, and one informal mechanism involving only a few parties—can allow for a pivot to firmer ground when one mechanism is not generating much traction.[49] This of course presumes that those involved know the options available to them, and the relative strengths and weaknesses of each.

Structural Gaps

Few efforts to maintain and share lessons learned

In both government and industry, Stimson found that new initiatives to facilitate public-private coordination often failed to iterate on previous efforts. Cross-functional initiatives, in which more than one professional/subject-matter COI was represented, were particularly susceptible in this regard. To an extent, this makes sense, as a single COI by definition has a shared history and shared conceptual approaches that allow them to identify problems and next steps more easily. But it also is sobering, because many of the security challenges that will compel public-private approaches in the years ahead will require disparate COIs to pool capabilities and expertise.

In public remarks at a June 2012 panel discussion, Angela McKay of Microsoft's Global Security Strategy and Diplomacy team described four "phases of maturity" that she saw unfold first-hand in public-private collaborations:

1. ***Recognizing the need for a joint effort***, with at least one government and one industry entity working on a common problem set.
2. ***Defining roles and responsibilities*** for a cooperative effort through basic mutual education, as well as exercises/simulations and similar steps.
3. ***Re-scoping the effort*** to a more focused, discrete space once it is clear how the effort is oriented to related initiatives.
4. ***Scaling the effort*** so that the solutions developed have greater reach but the associated processes do not become overly rigid and thereby stifle progress.

The problem, Ms. McKay added, was that many efforts over the years essentially had to reconstruct this road map from scratch, with participants proceeding in fits and starts. If they had known how their cooperation and scope of effort were likely to evolve, she said, it would have made a meaningful difference.[50]

Another important point embedded in Ms. McKay's model—essentially a corollary of her description of phase four—is the need for what we might call a preliminary "operational planning" phase. In other

[49] We thank an interviewee from the dual-use technology space for this insight.

[50] Angela McKay, public remarks, Center for Strategic and International Studies, Washington, DC, June 22, 2012.

words, *before* embarking on any cooperative effort, it would be useful for all parties to gain a better understanding of the different *modalities* that could shape their interactions—from informal to highly formal—along with their relative advantages and disadvantages. Moreover, this preliminary phase would provide situational awareness of any related initiatives already underway, along with ideas for how a new effort might complement or otherwise connect to those other initiatives. Developing an "operational plan" in this manner responds to the strategic imperative we discussed just above—the need for public-private relationships themselves to be "risk-managed" by identifying multiple potential objectives and the associated paths forward.

Stovepiping in both government and industry

The need for greater interagency cooperation is clear in many contexts. What is somewhat rare amidst all the admonitions is quantified evidence of how poor coordination endangers security and economic competitiveness. A March 2013 article on the new Export Enforcement Coordination Center (E2C2), established as part of the administration's export control reform effort, provided such evidence.

The article documented several cases in which multiple agencies independently had been investigating trade violations or security threats, until the E2C2 flagged the potential for self-inflicted setbacks and established better situational awareness for all involved. In all, by integrating case files from multiple agencies and cross-referencing target names with other data stores, such as phone numbers, the E2C2 found that about 60 percent of USG targets were being pursued by multiple agencies.[51] In the large majority of cases, the agencies had no knowledge of this wasteful and potentially counterproductive duplication.[52] We are hopeful that discoveries like this encourage more unity of effort at higher levels of the departments and agencies shown to be complicit in such uncoordinated operations.

With regard to the day-to-day operational needs of industry, a major problem is that 48 agencies have separate filing requirements for US importers and exporters, and some of the electronic interfaces they use are terribly antiquated and are not interoperable. (To be clear: The number of agencies with which any single company must file depends on the number and kind of products being imported/exported, as well as the location and identity of its trading partners.) Some agencies in the maritime space still require thick stacks of paper for each individual shipment. Congress mandated streamlining of these processes in the 1993 Customs Modernization Act (part of PL 103-182), and implementation of that mandate took shape under the umbrella of the Automated Commercial Environment (ACE).

Two decades later, ACE is incomplete. Only recently did work begin on incorporating data from beyond CBP into the most important component of ACE: the International Trade Data System (ITDS). ITDS is to serve as industry's "single window," which is to say the vehicle to consolidate filing requirements from the 48 agencies noted above. The plodding pace in making ITDS fully operational has meant that true "account management"—in which the USG, working on a whole-of-government basis, can assess and incentivize a company as a whole enterprise—has not yet even had a fighting chance. In the words of the American Association of Exporters and Importers (AAEI): "[T]he single most significant stumbling block to progress is the current state of the ACE."[53]

---

[51] Communications providers are one of the many "facilitators" whose activities can reveal dispositive network ties when traditional investigative and analytic methods cannot.

[52] John Shiffman, Reuters, "New Anti-Smuggling Center Uncovers Internal Surprises" (March 6, 2013). Online at http://www.reuters.com/article/2013/03/06/us-usa-smuggling-idUSBRE9251FV20130306.

[53] AAEI, comments submitted to House Ways and Means Committee, Subcommittee on Trade, for hearing on "Supporting Economic Growth and Job Creation through Customs Trade Modernization, Facilitation, and

All of this amounts to a major drag on economic competitiveness—and represents *a critical missed opportunity for the USG to leverage an integrated set of historical and near-real-time trade data for missions related to national security and trade violations (such as IPR infringements)*. While the Trade Act of 2002 created a "firewall" between commercial and security-related trade data, leading industry figures have expressed support for the addition of "commercial targeting" to the permitted uses of security data.[54]

Even the USG's more affirmative steps to work with industry are hampered by stovepipes. One need only look at the sheer number of USG advisory committees, working groups, and other bodies aiming to facilitate industry outreach. Recalling the four phases of maturity for public-private engagements articulated by Angela McKay, outlined just above, we can say that there is legitimate value in creating separate mechanisms to focus on a particular problem space. But as Ms. McKay emphasizes in her third phase, these multiple mechanisms deliver greater value only when they are coordinated—or at least basic awareness of one another. Stimson found that this coordination typically is weak.

Many departments and agencies have earnestly sought to streamline and strengthen their industry engagement through higher-level reviews. A 2012 Defense Business Board (DBB) report marks a notable effort for DoD.[55] As in the DBB report, the scope for most of these assessments does not extend above the department level. But the USG organizational chart, to put it mildly, does not correspond neatly with private sector networks in general or transnational commercial networks specifically. It remains possible that the USG could derive additional value from these department-level studies through a comparative analysis to identify both gaps and redundant efforts.

Stimson found that industry suffered from stovepipes of its own. A fairly common problem was that communication across functions or across communities of interest (COIs) was either infrequent or significantly inhibited by different cultures and objectives. We saw this across firms and, sometimes, even within firms. Indeed, in the area of trade controls, it is almost a truism that a company's chief compliance officer operates in a different environment and pursues different goals than the same company's chief sales officer.

Similar to the government-industry challenges discussed above, then, the cross-boundary communication problem within industry is not altogether unexpected. But it does have an important implication for government-industry cooperation: Government is likely missing many opportunities for additional private sector support of its security objectives by engaging only limited constituencies among a larger pool of potential private sector interlocutors. "Industry" is far from monolithic.

One specific manifestation of cross-functional separation within industry merits special attention. Within companies—and essentially at any level of analysis one wishes to consider—we found a significant disjuncture between information risk/security officers on the one hand, and most other functional units and COIs on the other. For instance, and to the particular question at hand, we saw limited evidence within industry that information security specialists had anything approaching a "common language" with subject matter experts in the CBRN domain.

Casual observers might not think this kind of disjuncture would have tangible or direct consequences. But with the growing centrality of the cyber domain in global economic and security dynamics, this is an area

---

Enforcement" (May 17, 2012). Online at http://www.aaei.org/LinkClick.aspx?fileticket=Bk%2BzzgGI3os%3D&tabid=36.

[54] See, e.g., NAM Vice President Vargo's testimony (see note 46), p. 8.

[55] Defense Business Board, "Public-Private Collaboration in the Department of Defense" (2012). Online at http://dbb.defense.gov/pdf/FY12-04publicprivatecollaborationDOD_0984.pdf.

where improvement should be an urgent strategic priority within companies, within industries, and in government-industry engagements. Here again, the nexus of IPR and information security might be common cause for all concerned.

Solutions from Industry: Building an Agile Framework for Sustainable Cooperation

Key Takeaways for the USG

Set the right tone in industry engagements with these three messages

Let there be no confusion: For industry, tangible outcomes are paramount. That of course is why the issue of incentives is so important. But in listening to our private sector participants, it became clear that narrative and tone do matter for public-private engagements. In more practical terms, narrative and tone can significantly affect prospects for tangible outcomes. This was especially true in cases where industry felt that previous attempts to work with government had failed to deliver.

We have attempted to capture the high-level themes or "frames" that resonated most with industry, across sectors. They are presented here in three notional messages that should inform how government approaches its industry interlocutor(s), either before or during a public-private initiative.

What Would Industry Like to Hear from the USG?*

1. **Incentives that matter. . .**

   "The USG will consider a more diverse, more industry-relevant, more practically implementable set of incentives for coordinated security efforts—if you help us identify those incentives."

2. **Different business models, different USG approaches. . .**

   "*We recognize that 'one size does not fit all.' Help us ensure that we design our joint efforts in a way that reflects the specific business models of participating private sector actors, as well as the specific security goals of government. When we can build on an existing effort to the benefit of all involved, we will."*

3. **"Account management," reinvented. . .**

   "To the maximum extent possible, the USG will take an 'end-to-end' view of your company's strategic and operational environments, and of all interactions between your company and all USG components. Ultimately, we want you to help us re-invent 'account management,' on a government-wide scale."

* To be clear: What we articulate here are merely stylized, hypothetical statements that a USG representative could deliver in dialogue with industry representatives. These statements capture, in spirit and in substance, high-level industry preferences.

As these themes started to crystallize for the Stimson project team, we vetted them with select industry figures. On the whole, these individuals expressed strong agreement that the three messages above would go far in establishing a more constructive tone and shaping more mutually beneficial outcomes. What was

especially notable, however, was how engaged these individuals were when we posed this question to them. Stepping back to think through big-picture issues of tone and process was not a luxury most of them had—and perhaps not an exercise that they would have considered useful, before being pressed.

Several even said it would be useful to undertake a more extensive, more iterative effort to elaborate on such a list, yielding a sort of "framework of principles" for public-private mechanisms. One person suggested that a widely endorsed framework like this could then be adapted at the outset of any new initiative, with more granular statements for the given problem space (e.g., supply chain integrity) nested within the big-picture themes.

These ideas are not to be mistaken as an exercise in branding. Upon conveying such messages to industry, a USG component would have a finite window to translate words into action. Prolonged delay would be tantamount to a lost opportunity. This danger is one reason why we frame the messages with a degree of interaction and shared responsibility built in. The other reason we do so, of course, is that government simply will not be able to achieve by itself the embedded goals of capturing specific business model characteristics, identifying relevant and meaningful industry incentives, and so on—to say nothing of the ultimate national security objectives.

Enhance understanding of industry landscape

How might government actually deliver these messages with credibility? And what comes next?

Our private sector participants told us on several occasions that one answer to both questions could be found in a more thoroughgoing and consistent effort by government to learn about the industry landscape. There already are several examples in the supply chain security space where the USG is taking on this challenge. For example, the National Customs Brokers and Forwarders Association of America (NCBFAA) recently established a series of education seminar for senior CBP officials. NCBFAA says that the goal is to help CBP better understand the "the functions and capabilities of a customs broker so that this expertise can be better leveraged by CBP," even though the customs broker "must direct his primary loyalty" to his client, the US importer.[56]

While brokers (and freight forwarders on the outbound side) might strike some as playing unremarkable "middleman" roles, the NCBFAA initiative matters. Brokers and freight forwarders are increasingly influential in the modern economy, even if their growth prospects are uneven.[57] (In fact, one could argue that difficult economic periods heighten their profile in the security conversation even further.) They are a window onto many of the other "facilitators" we cited earlier as key to understanding both licit and illicit trade. Couple that with ongoing changes *within* the transport/supply chain space, and the implications for law, regulation, and security are significant.[58] In the words of NCBFAA President Darrell Sekin, "A customs broker assumes a special, unique place in accomplishing [CBP's] mission."[59]

---

[56] Testimony of Darrell Sekin Jr. (President, NCBFAA) before the House Ways and Means Committee, Subcommittee on Trade, on "Supporting Economic Growth and Job Creation through Customs Trade Modernization, Facilitation, and Enforcement" (May 17, 2012), pp. 2-3. Online at http://waysandmeans.house.gov/UploadedFiles/Sekin_Testimony.pdf.

[57] See, e.g., Rob Knigge, "Freight forwarding and logistics: What the high performers know," Accenture Outlook (January 2013). Online at http://www.accenture.com/us-en/outlook/Pages/outlook-online-2013-freight-forwarding-and-logistics-what-high-performers-know.aspx.

[58] Finlay/Olson interviews (2012-2013).

[59] Sekin, p. 1.

Whatever the issue and whomever the participants, the structure and setting for less formal initiatives do deserve scrutiny. It might benefit the principal actors on both the government and industry sides for such initiatives to be convened by a third party with sufficient knowledge of—but not a vested interest in—the relevant industry and regulatory variables. A trusted third-party facilitator also can help such dialogues endure beyond a one-off meeting or navigate through especially difficult discussions.

Two other CBP outreach initiatives hold particular relevance for USG awareness of industry dynamics. One is establishment of the Centers for Excellence and Expertise (CEEs), a new model for oversight of US imports. The CEEs are sector-specific and mostly virtual organizations in which a central office patches in CBP's top industry experts when a relevant import-related issue arises, then broadcasts their assessment to all US ports of entry. In so doing, the CEEs aim to provide participating US importers faster and more consistent CBP decisions on clearing cargo for entry.

It bears mention here that the CEEs are one product of a new, overarching concept for industry engagement that CBP is aggressively publicizing. CBP calls it "co-creation." While there is no precise definition for the term, co-creation is part process and part ethos. It involves working with one or more stakeholder groups to iteratively design, implement, and maintain a product or service. The term is borrowed from the management consulting world, which used it first in business-to-consumer and business-to-business (B2B) relationships. Some of the most common B2B applications center on supplier relationships and supply chain management more broadly.[60] While some might deride CBP's use of the term as window-dressing, Stimson's feedback from industry leads us to reserve judgment. One Stimson interviewee called the CEEs a "ray of hope" amidst an often-frustrating relationship with CBP. More broadly, CBP deserves

The CEEs also are focal points for CBP to gather what it calls "trade intelligence"—essentially all manner of information that CBP could use for targeting, enforcement, or broader situational awareness. Thus far, the trade intelligence function has been deployed at two CEEs: the electronics CEE in Los Angeles, and the pharmaceuticals CEE in New York City. [61]

The second CBP outreach effort, also branded as "trade intelligence," is the Private Sector Industry Liaison Office (PSILO). The PSILO identifies suitable industry contacts within the customs compliance, security, and supply chain sourcing departments of firms and trade associations. According to CBP, those representatives will then "provide critical insight to CBP on enforcement issues related to developments in the [IPR], anti-dumping and countervailing duty, and trade preference areas, as well as advise CBP on the latest industry-wide changes."[62]

While the industry representatives and CBP officials are not physically co-located, what this initiative is attempting (both in kind and in degree) certainly will test boundaries in several respects. For instance, it will be intriguing to watch for any notable dissension between companies that are taking part in the PSILO concept and those that are not. As to the governance and accountability dimension, it must be noted that CBP is making no secret of this effort—but all the same, now is an appropriate time to raise the role of Congress. USG offices contemplating any sort of unconventional initiative along these lines in

---

[60] See, e.g., PwC's PRTM Management Consulting and its portrayal and use of the concept at http://www.prtm.com/strategiccategory.aspx?id=4100&langtype=1033

[61] See, e.g., http://www.cbp.gov/linkhandler/cgov/trade/trade_transformation/tt_2012_accomp.ctt/tt_2012_accomp.pdf, http://www.cbp.gov/xp/cgov/trade/trade_transformation/industry_int/, and http://www.cbp.gov/linkhandler/cgov/trade/trade_transformation/external_trade_trans.ctt/external_trade_trans.pdf

[62] CBP, "Fact Sheet: Trade Intelligence" (July 2012), online at http://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/trade/ttfs/tradeintelligence.ctt/tradeintelligence.pdf

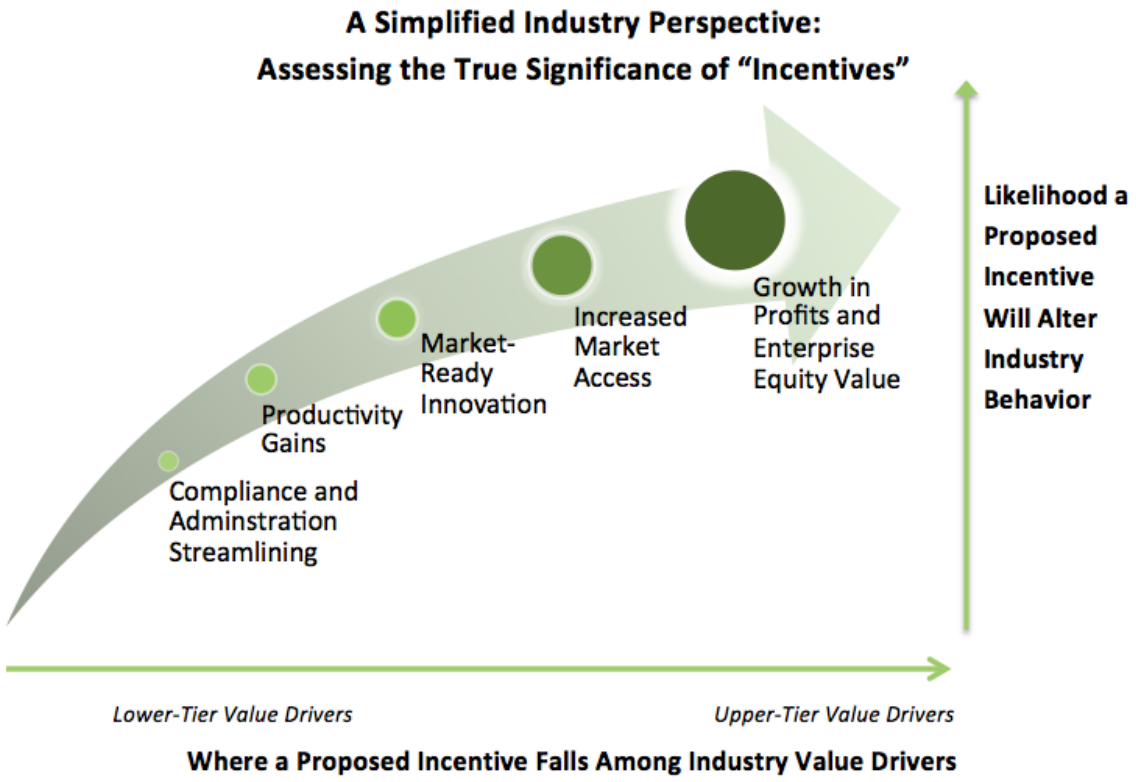
their private sector outreach—especially one that will not be in the public eye regularly—would do well to seek congressional input early and often.

Bring the full spectrum of industry's value drivers into view

To what end should such outreach mechanisms and other educational efforts be directed? One major need is now clear to Stimson: ***Government must significantly enhance its knowledge of the full spectrum of value drivers for its industry interlocutors.*** This is part and parcel of developing a well-rounded understanding of contemporary global economic networks, as already emphasized. But it also is a fundamental prerequisite to identifying what incentives can elicit meaningful industry engagement in security dialogues.

Figure 4 depicts a simplified view of how industry evaluates any given government-proposed incentive against its full range of value creation opportunities. This depiction is based on input from one of Stimson's industry participants. The simple but striking fact is that most of the public-private narrative on incentives for security coordination is anchored in the lower left portion, the compliance and administration area.

FIGURE 4[63]



In large part, this compartmentalized thinking appears to have its roots in the same stovepiping and communication challenges we highlighted above. Most government officials tend to deal with a limited breadth of issues in their work, and their mental models for those issues have a similar scope and orientation. To the extent their work involves communicating across the public-private divide (e.g., on

[63] Stimson thanks one of its industry interlocutors for the ideas that led to this visual.

customs matters), the substance of those interactions likewise does not typically depart from a limited range—the transactional, business-as-usual range. These are dangerous tendencies for a government that wants to leverage private sector advantages in a fast-paced market environment. The USG must think more expansively about how it can fashion incentive structures that transcend the transactional level.

To illustrate, let us focus on just one of the higher-level value drivers in our visual: innovation. Some of our industry participants voiced dismay that potential commercial applications of USG-funded technologies did not figure more prominently in their conversations with government. Some in government might not see the merit or potential for technology transfers. But it is important to realize how rapidly and effectively industry can extend and rejuvenate the innovation cycle.

One instructive story in this regard is the commercialization of Global Positioning System (GPS) capabilities. The US steadily increased GPS functionality for civilian and commercial use after the end of the Cold War, with a major breakpoint coming in the Clinton administration's March 1996 policy statement.[64] While hopes were high, consider how uncertain the exact prospects for GPS were at the time—even to those well acquainted with its underlying technologies and the contemporary business environment:

> "Like other information-based technologies, the generic applicability of GPS makes it an enabler of productivity improvements through reducing costs, enabling new functions, or enhancing revenues. The economic benefits of civil and commercial applications of GPS are thus broader than might be measured by sales of GPS equipment and service-related sales alone. At the same time, projecting future benefits is uncertain at best—it is difficult to predict where GPS-dependent productivity benefits might be found in the economy. Lowering the cost of using GPS is seen by industry as a crucial aspect for the growth of GPS, not only in terms of increasing demand from people who know what they want to use GPS for, but also in terms of encouraging experimentation with GPS by persons who are not sure if it will be useful." [65]

As the conclusion of this passage notes, technology transfer can enable a virtuous cycle of innovation, even if immediate private sector applications are not apparent. Initial innovations, though modest, can drive costs down to the point that a technology reaches critical mass among interested firms. The broader experimentation makes substantial breakthroughs more likely.

A more comprehensive framing of industry value drivers is also a fitting backdrop against which to reiterate our earlier point about intellectual property and information security. Intellectual property is a tremendous store of value for many US firms—a resource to defend, yes, but also a resource to proactively leverage for new growth. The USG advances both public and private sector interests when it empowers trusted partners in industry to put potentially valuable knowledge or technology to productive ends, and when it helps create secure channels to share information around the world. Indeed, the free flow of information across borders will be increasingly vital.[66] There are several projects and programs across government that provide positive examples in this regard.[67]

---

[64] Office of Science and Technology Policy, "Fact Sheet: U.S. Global Positioning System Policy" (March 29, 1996). Online at http://clinton4.nara.gov/textonly/WH/EOP/OSTP/html/gps-factsheet.html.

[65] Scott Pace et al., *The Global Positioning System: Assessing National Policies* (RAND, 1995), p. 103. Online at http://www.rand.org/pubs/monograph_reports/MR614.html.

[66] See, e.g., National Foreign Trade Council, "Promoting Cross-Border Data Flows: Priorities for the Business Community" (November 2011), online at http://www.nftc.org/default/Innovation/PromotingCrossBorderDataFlowsNFTC.pdf

[67] See, e.g., the DHS SECURE and FutreTECH programs as discussed in Thomas Cellucci, "Innovative Public-Private Partnerships: Pathway to Effectively Solving Problems" (July 2010), online at

Diversify the USG "portfolio" of outreach tools and modalities

As emphasized earlier, it is crucial that government be able to draw on a fuller set of tools in working with industry, underpinned by a better understanding of what has and has not been effective in past efforts. Part of the work here is learning the comparative advantages of different modalities, particularly as they are suited to the relevant mission area.[69] But a more fundamental task is establishing a capability to capture those lessons and put them in a broader framework.

To this end, the perspectives of industry figures with substantial experience in public-private efforts are highly valuable. Further work to collect their views and identify major themes is imperative. To combine several of the threads from above: Industry figures who have worked in cross-functional settings on a problem involving information risk, or secure information-sharing, deserve particular focus. Moreover, any past effort that has succeeded in breaking down stovepipes in either government or industry and spurring cross-functional problem solving should be carefully examined.

Noteworthy Antecedents and Current Efforts: USG

Stimson's private sector interlocutors noted many past or ongoing initiatives that they felt merited the attention of USG audiences. We present a selection of these—some USG-led, some industry-led—that we feel noteworthy, though the precise reasons for highlighting each one differ.

National Strategy for Global Supply Chain Security (NSGSCS) implementation tracks

Several elements of the NSGSCS implementation effort are directly relevant to CBRN mission areas, to the industry desire for enhanced trade facilitation, and to the more general USG-wide effort to forge better industry cooperation. Areas of focus for 2013 include:

- "[Development of] a 'United States Government Supply Chain Partnership Program Framework' to inform Federal departments and agencies as they work to develop new supply chain partnership programs, or to refine existing ones to improve harmonization or achieve mutually [*sic*] recognition of requirements."[70]
- "[Refining] and [utilizing] risk assessments, such as the Radiological/Nuclear Global Supply Chain Risk Assessment, to inform the deployment of technical solutions and other capabilities… to strengthen the Global Nuclear Detection Architecture and related national policies and programs."[71]
- "Developing and launching a global partnership on supply chain risk and resilience."[72]

---

http://www.dhs.gov/xlibrary/assets/st_innovative_public_private_partnerships_0710_version_2.pdf. See also the National Digital Engineering and Manufacturing Consortium (NDEMC) at http://ndemc.org.

[69] See, e.g., Linton Wells II and Samuel Bendett, "Public-Private Cooperation in the Department of Defense: A Framework for Analysis and Recommendations for Action," *Defense Horizons* no. 74 (National Defense University, October 2012), online at http://www.ndu.edu/CTNSP/docUploaded/Defense%20Horizons%2074.pdf; see also William Tobey, "Defining and Implementing Best Practices in Nuclear Security," Discussion Paper #2012-13 (Belfer Center for International Affairs, December 2012), online at http://belfercenter.ksg.harvard.edu/files/William_Tobey_Defining%20and%20Implementing.pdf.

[70] "NSGSCS Implementation Update" (January 2013), p. 20. Online at http://www.whitehouse.gov/sites/default/files/docs/national_strategy_for_global_supply_chain_security_implementation_update_public_version_final2-26-131.pdf.

[71] *Ibid*., p. 9.

[72] *Ibid*., p. 10.

National Information Exchange Model (NIEM): CBRN and maritime domains

One mechanism quite far down the "formal" end of the spectrum is the NIEM, managed by the Program Manager for the Information Sharing Environment (PM-ISE). Pursuant to the Implementing Recommendations of the 9/11 Commission Act of 2007 (PL 110-53), the PM-ISE has

The NIEM provides standardized vocabularies to facilitate information-sharing for a variety of purposes, and by many different communities of interest (COIs). It has been expanded over time as different COIs have contributed their expertise to create subject-specific "domains," or sets of data elements and their corresponding relationships. As of early 2013, there are 15 fully mature domains, including the CBRN and maritime domains.

The development of the CBRN (ChemBioRadNuc) domain is the culmination of a long-term effort to increase data harmonization. This effort has created the N.25 Protocol, which is a standard messaging service that disseminates information exchange messages regarding the transfer and processing of nuclear materials.[73] As part of the Global Nuclear Detection Architecture, the NIEM extends to a variety of organizations, including the Departments of Homeland Security, Justice, Energy, State, Defense; the Nuclear Regulatory Commission; and other local and state agencies.[74] The system is stewarded by the Domestic Nuclear Detection Office (DNDO).

CBRN-related information from a variety of sensors is fed through the Joint Analysis Center (JAC). According to a DNDO data analyst, "The JAC doesn't control or operate anything in the field, but they're an important source of knowledge: wiring it all together so the dots can be seen, and then figuring how you're going to connect the right dots."[77] The advantage of this system, then, is the ability to transmit and disseminate information regardless of the original sensor.

Before adopting NIEM, the DNDO relied on inconsistent data sharing programs. E-mail and other inefficient transmitting systems were used to disseminate threat intelligence. Information was poorly coordinated, and the various systems used were not interoperable.[78] Moreover, human error was a major concern. Because of this inefficiency, especially in dealing with complex sensory data, a new and unified system was needed. DNDO did not think NIEM 1.0 was a viable option for handling the complex scientific data the CBRN community required. However, DNDO saw NIEM 2.0 as a major upgrade and adopted it.

DNDO initially piloted NIEM 2.0 in 2008 through the Southeast Transportation Corridor Pilot (SETCP).[79] This initiative proved successful and illustrated three vital advances: first, it demonstrated that the DNDO authored messages would be supported by NIEM; second, it showed that non-experts could produce NIEM-conformant messages quickly; and third, experts could interpret these messages when they were sent machine-to-machine.[80] "Most important, perhaps, in SETCP, DNDO demonstrated that a vastly distributed network of networks might soon carry messaging alerts from sensors to analysts to

[73] W.R. Wright, "Interoperability Standards and Capabilities for Global Nuclear Detection Architecture," presentation to the Workshop on Information Sharing and Safeguarding, December 5, 2011. Online at http://www.ise.gov/sites/default/files/Track4-BillWright-WIS3-InteroperabilityStandardsandCapabilities.pdf

[74] https://www.niem.gov/communities/cbrn/Pages/about-cbrn.aspx

[77] http://www.ise.gov/sites/default/files/DNDO-Brochure_20110705.pdf

[78] *Ibid.*

[79] *Ibid.*

[80] *Ibid.*

operators, no matter where or when they were received, and that it could do so with astonishing speed and accuracy."[81]

While the NIEM CBRN domain has improved information exchange amongst domestic institutions, experts agree that international integration of the NIEM is necessary. Trade with Canada and Mexico necessitates similar integration for a more streamlined process. The DNDO is increasingly partnering with international organizations, including the IAEA, to strengthen the global nuclear detection architecture.[82] The Practical Arrangements for Cooperation between DHS and the IAEA outlines how the organizations collaborate on standards, testing, characterization, and evaluation for nuclear detection instruments.[83]

NIEM's maritime domain took root in late 2008 when the NIEM program office and DoD agreed that it would be synchronized with future development of the Maritime Information Exchange Model (MIEM). The MIEM was developed under the Comprehensive Maritime Awareness Joint Capability Technology Demonstration. It is "aimed specifically at developing and demonstrating effective means for sharing maritime intelligence to improve interdiction of suspicious or threatening vessels, cargo, and people."[86] MIEM messages convey nine areas of value added information: sensor system reports, caveats and simple metadata, fused data and inferred beliefs, degree of belief and pedigree, multiple alternatives and analysis, history and future projections, watch lists, threats and anomalies, and case files for key entities.[88]

While the MIEM has developed into a successful interagency tool,[89] there is a need to increase civilian input into the system.[90] Experts have said that the MIEM allows for both military and civilian exchange, but some say that there is much more value that could be derived from additional private sector data.[91]

Information Sharing and Analysis Centers (ISACs)

The ISACs are quasi-governmental in that they have special relationships with law enforcement and intelligence officials, but they are industry-led and serve principally to share "accurate, actionable, and relevant information" with private sector owners and operators of critical infrastructure.[92] The framework for ISACs was outlined under President Clinton in Presidential Decision Directive 63 (PDD-63), but their role dramatically increased with the December 2003 release of Homeland Security Presidential Directive 7, which updated PDD-63.[93]

While technically independent from the government, ISACs bring together information from a variety of sources, including the private and public sector. Each ISAC disseminates the information to its clients

---

[81] *Ibid.*

[82] http://www.dhs.gov/blog/2013/01/18/dndo-facilitates-international-strengthening-global-nuclear-detection-architecture

[83] http://www.dhs.gov/blog/2012/08/10/iaea-practical-arrangements-cooperation

[86] Donna Roy, "NIEM Program Partners with DoD to Support Maritime Information Exchange" (November 25, 2008). Online at https://www.niem.gov/documentsdb/Documents/Other/MIEM_Partner.pdf.

[88] Rick Hayes-Roth; David Reading. "Maritime Information Exchange Model" (September 29, 2008), online at http://faculty.nps.edu/fahayesr/docs/MIEM%20overview%20with%20notes%2020080929..

[89] http://www.ise.gov/sites/default/files/UCORE_NIEM_Success_Story_20100421.pdf

[90] Department of Defense. Executive Agent for Maritime Domain Awareness. "Maritime Information Exchange Model (MIEM) and National Information Exchange Model (NIEM) Transition," (2009), online at http://www.public.navy.mil/dodeaformda/FactSheets/MIEM-NIEM%20Fact%20Sheet%20vr4%20_2_.pdf

[91] Hayes-Roth and Reading, "Maritime Information Exchange Model."

[92] http://www.isaccouncil.org/aboutus.html

[93] https://secure.sc-investigate.net/SC-ISAC/ISACAbout.aspx

through variety of services, which are often tailor made for the specific industry. These services range from 24/7 security operations centers, threat and risk assessments, and periodic debriefings.

ISACs do function independently, but the National Council of ISACs, established in 2003, provides a forum where ISAC leaders can meet one another and government representatives to discuss security issues. In addition, during emergencies, they receive classified briefings from the Department of Homeland Security's National Infrastructure Coordinating Center.

A select number of individual ISACs are described below:

> ***Financial Services ISAC:*** The FS-ISAC is often said to be the most active and organizationally innovative ISAC. It focuses heavily on cybersecurity and other issues related to information risk. Over the past decade, it has developed the Critical Infrastructure Notification System, which anonymously disseminates threat information to FS-ISAC member companies.[95] Notably, the FS-ISAC is the only ISAC with an international membership.
>
> ***Maritime ISAC:*** M-ISAC plays a role in protecting the security of the maritime industry. It acts as an information-exchange hub for member companies and identifies major physical security threats, including stowaway and trafficking levels, drug seizures, and terrorist and piracy threats.[97]
>
> ***Information Technology ISAC:*** IT-ISAC has two broad functions, both of which improve security within the IT sector. First, IT-ISAC has created an information exchange network both within private industry, and between private industry and the government.[98] This network, with information provided by both sectors, allows IT-ISAC to inform member companies of current threats and attacks. Second, IT-ISAC acts a liaison between private industry and the US and international policymakers, in order to create smart policy regarding IT security.
>
> ***Supply Chain ISAC:*** SC-ISAC was formed in 2006 in order to better coordinate threat information submitted by member companies, law enforcement and various government agencies. Like the other ISACs, SC-ISAC's main focus is analyzing pertinent information on emerging threats, and disseminating it to member companies.[101] This information web creates a vital network that protects and informs a large swath of critical industry, including shippers, cargo carriers, consignees, and supply chain service suppliers.[102] SC-ISAC operates a secure, 24/7 operations center..

CBP "co-creation" efforts

We noted above that the Centers for Excellence and Expertise (CEE) were one product of CBP's co-creation model. Another initiative that CBP often highlights in this regard is the Air Cargo Advanced Screening (ACAS) program. ACAS took shape in the immediate aftermath of the attempted "printer cartridge bombing" of two express delivery air cargo flights. Executives from the express air carriers conferred with DHS leadership and soon developed a proposal for improvements to advanced data-sharing for air cargo. That proposal grew into an ACAS pilot initiative. DHS is now in the process of formalizing the program.

---

[95] https://www.fsisac.com/about/committees

[97] Ibid.

[98] https://www.it-isac.org/about_n.php

[101] https://secure.sc-investigate.net/SC-ISAC/ISACFAQ.aspx

[102] Ibid.

Department of Commerce Technical Advisory Committees (TACs)

The TACs bring together government, industry, and academic interlocutors to discuss the administration and technical aspects of export controls for dual-use commodities and technologies. There are eight TACS in all: Emerging Technology and Research; Information Systems; Materials; Materials Processing Equipment; the President's Export Council Subcommittee on Export Administration; Regulations and Procedures; Sensors and Instrumentation; and Transportation and Related Equipment. Committee members serve four-year terms. The functions and activities of the TACs are governed by the Federal Advisory Committee Act (FACA). Those in the CBRN community might wish to pay special attention to the work of the following TACs:

> ***The Emerging Technology and Research Committee (ETRAC),*** whose work is somewhat different from the other TACs. Its objective to identify emerging dual-use technologies, create a list of potential controls, predict the outcomes of the controls, and use the information to assess the overall national security threat of unauthorized export controls of dual-use technologies.[103]
>
> ***The Materials TAC***, which concentrates on materials that may be used to develop nuclear, chemical, and biological weapons, as well as materials, articles, and supplies for radar absorption, jet engine turbines blades, super-conductivity, fluids, lubricants, and composites.[104]
>
> ***The Materials Processing Equipment Committee***
>
> ***The President's Export Council Subcommittee on Export Administration (PECSEA)***, which is one part of the USG's main advisory committee on international trade matters. The PECSEA is undertaking a global benchmarking study of other national export control regimes. The objective is to highlight additional mechanisms and processes that governments use for effective trade controls, in addition to the traditional license.[105] The PECSEA also is a key source of private sector feedback on the ongoing export control reform initiative (ECR). That role is likely to take on heightened importance in the next 1-2 years, as the ECR effort shifts its focus from the US Munitions List to the Commerce Control List. The latter contains dual-use items whose trade is regulated by the Department of Commerce's Bureau of Industry and Security. (The State Department's Defense Trade Advisory Group, or DTAG, is the primary vehicle for industry to provide its views on issues related to the US Munitions List.[106])
>
> ***The Sensors and Instrumentation Committee***[107]

Noteworthy Antecedents and Current Efforts: Industry

Nuclear Power Plant Exporters' Principles of Conduct (POC)

The POC is a private industry code of conduct, outlining norms of corporate self-management in the export of nuclear power plant technology. Many of the world's leading nuclear power plant vendors have signed on. The POC was the product of a three-year effort that started in October 2008, under the leadership of the Carnegie Endowment for International Peace.

---

[103] http://tac.bis.doc.gov/etracchart.htm

[104] http://tac.bis.doc.gov/

[105] Finlay/Olson interviews (2012-2013)

[106] See http://www.pmddtc.state.gov/DTAG/

[107] http://tac.bis.doc.gov/sichart.htm

The POC encompass a wide gamut of norms relating to the exportation of nuclear power-plant technology, including safety, nuclear security, environmental protection, compensation (for nuclear damage) and non-proliferation. As of early 2013, the following companies have adopted the POC:

- AREVA
- ATMEA
- Babcock & Wilcox
- Candu Energy
- GE Hitachi Nuclear Energy
- Hitachi-GE Nuclear Energy
- KEPCO
- Mitsubishi Heavy Industries
- Mitsubishi Nuclear Energy Systems
- Rusatom Overseas
- Toshiba
- Westinghouse Electric Company

The Coalition for Excellence in Export Compliance (CEEC)

The mission of the CEEC is to "identify and recommend export compliance best practices that provide practical guidance to better detect and prevent violations of law."[110] The group notes that there is no perfect set of export compliance procedures, but a more unified set will have benefits for both the government and the export industries.[111]

The CEEC is based on the premise that increasing the uniformity of controls will spur export confidence, providing more streamlined and efficient supply chains.[112] In addition, the written guidelines will provide government with a framework to better understand the export community and create a better working relationship.

The group has outlined eight areas of standards to ensure legal compliance. These standards provide the blueprint for export companies, outlining the necessary steps for ensuring compliance:

> ***Classification:*** The CEEC outlines the process that should be established to create appropriate export classification. They concentrate on uniform international classifications, and ensuring export occurs only if the product has been classified. Because classification is vital to export transparency, a well maintained and constructed classification database is a necessary component of the export model. [113]
>
> ***Disclosure:*** Companies must have a proper system of disclosure for violations of export laws. This process must be outlined in detail, both internally and with the government. Further, employees must be provided proper legal protection if they report violations. [114]

---

[110] "CEEC Best Practices For Export Controls." http://www.ceecbestpractices.org

[111] "CEEC Introduction." http://www.ceecbestpractices.org/best-practices-standards-workgroup.html

[112] Ibid.

[113] "CEEC Draft Working Group Standards: Classification." November 29, 2011. http://www.ceecbestpractices.org/uploads/9/1/2/6/9126226/ceec_-_classifications.pdf

[114] "CEEC Draft Working Group Standards: Disclosure." April 12, 2012. http://www.ceecbestpractices.org/uploads/9/1/2/6/9126226/ceec_disclosures_4_30_12.pdf

Intangible Exports: CEEC outlines the necessary controls for intangible exports (usually technical information). They cover the screening of hardware, and the movement of electric files. Intangible export control is crucial because they often are design sensitive. These standards aim to control not just the initial transfer, but also possible movement to third parties following export. [115]

Export Authorization Implementation and Use: These standards ensure that export is lawful. This includes guidelines that ensure adequate review of exports, correct authorization, and continuous record keeping. [116]

Screening: Ensures that UN and national government restricted lists are kept up to date and the companies' exports comply with these lists. This includes not exporting restricted items, as well as curtailing export to prohibited buyers.[117]

Management Commitment: Compliance is only as successful as the attention the senior management affords to the program. CEEC outlines 5 guiding principles necessary for the senior management: promoting connection between the companies' values and the export compliance program; actually engaging in the export compliance program; providing the resources for the effective implementation; periodically evaluating the compliance program.[118]

Personnel: Compliance relies not only on senior management engagement, but ensuring that company personnel are actually responsible. Companies must ensure the quality, proper quantity, and location of the personnel. Companies should not be understaffed, and should have employees with the capabilities to be effective administrators of compliance. [119]

Training: Besides ensuring the proper personnel, company employees must be trained and retrained in order to keep up to date with export laws and protocol. The standards outline how often proper personnel should be retrained. [120]

CEEC's mission is part of the effort to ensure global compliance for exporters. Their standards provide the necessary information, and begin to create consensus on the necessary protocol and business strategy needed to ensure legal export. While the actors in the private and public sector have not come to a uniform consensus, the CEEC standards provide a basis for discussion. For the time being the CEEC standards are benchmarks for companies, and a tool to better streamline export compliance.

---

[115] "CEEC Draft Working Group Standards: Intangible Exports." November 29, 2011. http://www.ceecbestpractices.org/uploads/9/1/2/6/9126226/ceec_-_intangible_exports.pdf

[116] "CEEC Draft Working Group Standards: Export Authorization Implementation and Use." November 29, 2011. http://www.ceecbestpractices.org/uploads/9/1/2/6/9126226/ceec_-_authorization_use.pdf

[117] "CEEC Draft Working Group Standards: Screening." November 28, 2011. http://www.ceecbestpractices.org/uploads/9/1/2/6/9126226/ceec_-_screening_28_nov_2011.pdf

[118] "CEEC Draft Working Group Standards: Management Commitment." November 28, 2011. http://www.ceecbestpractices.org/uploads/9/1/2/6/9126226/ceec_-_management_commitment.pdf

[119] "CEEC Draft Working Group Standards: Personnel." November 29, 2011. http://www.ceecbestpractices.org/uploads/9/1/2/6/9126226/ceec_-_personnel.pdf

[120] "CEEC Draft Working Group Standards: Training." November 28, 2011. http://www.ceecbestpractices.org/uploads/9/1/2/6/9126226/ceec_-_training_28_nov_2011.pdf

Responsible Care

Responsible Care is a global voluntary initiative for self-regulation of the chemical industry. Its main objectives are to improve the chemical industry's environmental performance, to improve its relationship with government, and to foster increased public trust.

Responsible Care was introduced in 1985 in Canada in direct response to several chemical accidents in Europe, Asia and North America. Producers at the time realized that industry-wide collective action had to be taken to restore and maintain the industry's public image.[121] Responsible Care has developed into an elaborate environmental management system that outlines guiding principles, a chemical referral website, a verification process, and six codes of practice. The codes of practice address these topics:

- **Community Awareness and Emergency Response**
- **Research and Development**
- **Manufacturing**
    - Applies to all aspects of manufacturing and operations for new and existing sites. Systems must be developed to cover plant design, construction and operation to protect employees, the community and the environment from harmful effects of chemical manufacturing.
- **Transportation**
    - Members must have programs that ensure the transport of chemicals minimizes the risk of accident and injury to the transporters, the public, and the environment. In addition, they must provide people situated along transport routes with information concerning any dangers.
- **Distribution**
    - Establishes standards and procedures, and provides training guidance for the storage and handling of chemicals and chemical products. Members may not buy from suppliers or sell to distributors and customers who do not comply with the code.
- **Hazardous Waste Management**

The codes related to manufacturing, transportation, and distribution are of particular interest for those aiming to advance supply chain security from other vantage points.

Over the past decade, Responsible Care has continued to evolve. The Responsible Care Global Charter, which seeks to harmonize, govern, and expand the principles globally, was adopted in 2004 and launched publicly at the first UN International Conference on Chemicals Management in 2006.

One of the program's elements is the Responsible Care Security Code. The Code's management practices address facility, cyber, and transportation/value chain security. These serve as the basis for company security vulnerability assessments (SVAs) that companies must conduct. If deemed necessary, security enhancements must be implemented under a strict timeline using approved methods. Furthermore, companies must obtain independent verification to prove they have completed the required physical site security measures identified during the SVA.

---

[121] As Jean Bélanger, President of the CCPA, observed, "If a paint company or a plating company does something wrong the headlines the next day will scream that chemicals have been wrongly handled and so we will all be tarred by the same brush." See J. Bélanger, Responsible Care: Developing a Promise, presentation to the First International Workshop on Responsible Care, European Chemical Industry Council, Rotterdam, 1991.

ISO 28000 series (supply chain security)

The International Organization for Standardization (ISO) is one of the world's most influential standard-setting bodies. ISO 28000 specifies standards for security assurance in the supply chain. The specification was developed to codify operational security within broader supply chain management, and to harmonize the elements of this standard with related standards such as ISO 9001:2000, ISO 14001:2004, and ISO 31000:2009, the latter of which (risk management standard) we mentioned earlier.

The new standard is designed to help mitigate risks to people and cargo at all stages of the value chain. In the words of ISO Secretary-General Alan Bryden: "Threats in the international market-place know no borders. The ISO 28000 series provides a global solution to this global problem. With an internationally recognized security management system, stakeholders in the supply chain can ensure the safety of cargo and people, while facilitating international trade, thus contributing to the welfare of society as a whole."[126]

ISO 28000 requirements can be applied by organizations regardless of their size or industry sector, and at any stage of the production or supply process. The standard includes provisions to:

- establish, implement, maintain and improve a security management system;
- assure conformity with security management policy;
- demonstrate such conformity; and
- seek certification/registration of conformity by an accredited third party organization.

In 2012, SGS Philippines became the first entity in the world to be accredited for ISO 28000 by the ANSI-ASQ National Accreditation Board (ANAB).[127]

Transported Asset Protection Association (TAPA) standards

TAPA designs standards for trucking and air cargo companies related to the protection of high value theft targeted assets (HVTT) in transit. The assets under this definition include, but are not limited to, electronic goods, pharmaceuticals, industry parts, and high-end consumer goods.[150] TAPA encompasses three major branches: TAPA AMERICAS, TAPA EMEA (Europe and Africa), and TAPA APAC (Asia and Pacific).

TAPA utilizes a certification program to verify standards compliance. Companies and insurers are increasingly citing TAPA certification as a prerequisite.[151]

The TAPA standards are broken down into three broad areas: freight security requirements (FSR), Trucking Security Requirements (TSR), and Air Cargo Security Standards (TACSS).[153] Each of these three has its own unique goals and standards, necessitating separate requirements and certification procedures. However, all three involve a review by TAPA affiliated auditors, and a ranking system that reflects their compliance with the standards.

---

[126] http://www.iso.org/iso/news.htm?refid=Ref1086

[127] http://www.sgs.com/en/Our-Company/News-and-Media-Center/News-and-Press-Releases/2012/08/SGS-First-Accredited-for-ISO-28000-by-ANAB.aspx

[150] http://tapaonline.org/index.php/about-tapa

[151] *Ibid.*

[153] http://www.tapaonline.org/index.php/standards9

Freight Security Requirements (FSR): FSR provides the standards to ensure safe transit, storage and the warehousing of assets. TAPA makes it clear that the standards outlined are for each facility, and the company can only reach TAPA-certification if all company facilities are up to par.[154] While the certification provides minimum standards, there is a consumer review process that rewards companies that go beyond the TAPA standards. The TAPA employs a three-level ranking system, based on consumer reviews and TAPA-approved audit evaluations. Thus the framework incentivizes continued compliance with the standards. The certification process evaluates the main areas of warehouse and transportation security.[155]

Sector-Specific Proposals

The project team was heartened that, in each of the four industry spaces engaged for this project, several participants—including companies, trade associations, and some related actors—signaled a willingness to continue working toward concrete demonstrations of the principles and ideas they had advocated. Some of the concepts they have proposed are sketched below, but we have omitted many particulars in observance of our pledge to withhold identifying information or other sensitive details. Moreover, since these concepts remain in the formative stages, they could evolve into different directions pending reactions from various stakeholders. But fundamentally, we would emphasize our confidence that USG components from the CBRN community, the customs and trade facilitation domains, and several other communities of interest have genuine opportunities to improve existing public-private mechanisms and to develop new ones that produce mutual gains.

Dual-use technology manufacturers

- Form an industry coalition or task force to build capacity among small and medium sized manufacturers requiring assistance with (1) adapting compliance processes as their products are migrated from the US Munitions List to the Commerce Control List, pursuant to export control reform; or (2) integrating protections against intellectual property theft at all stages of the value chain. The second work stream would be focused especially on firms that are considering international sales (exports) for the first time, or that only recently began exporting.
- Pilot a "trusted exporter" initiative with a small number of companies (with small, medium, and large firms all represented), for a limited number of their cross-border transactions. Verification of sufficient supply chain security processes would entitle a company to a license exception of five years for the relevant transaction (i.e., same end-user, same route), as well as other trade facilitation benefits. Consider industry-led process to define the benchmark security practices against which USG measures compliance.

Radiopharmaceuticals

- Pilot additional uses of the SAFE-BioPharma digital signature standard to demonstrate its value for intellectual property protection and mitigation of information risks.[163] Work with insurance companies to identify mechanisms for increased adoption.
- Pilot a "trusted exporter" initiative. (This concept was largely in line with the proposal put forward by the dual-use technology manufacturers above.)

---

[154] http://www.tapaonline.org/images/pdfs/fsr/2011-fsr-changes.pdf

[155] http://www.tapaonline.org/images/pdfs/fsr/2011-tapa-fsr-reqs-final.pdf

[163] For background on SAFE-BioPharma, see http://www.safe-biopharma.org.

Shipping

- Pilot several demonstrations of new cargo-scanning technologies, perhaps as part of the National Strategy for Global Supply Chain Security implementation.
- Work with insurance firms to identify how existing industry standards and metrics, such as those devised by RightShip, might be leveraged to enhance various aspects of maritime security.[164] Initial area of focus could be port facilities and cybersecurity.

Insurance

- Improve communication between information risk officers and underwriting officers by recruiting several of the latter to participate in FS-ISAC activities and through other means. Develop best practices for cross-functional communication.
- Assist in development of the Cybersecurity Framework with the goal of designing coordinated products for information risk ("cybersecurity insurance").[165]

Conclusion

The clear limitations on governments' reach and the growing importance of the private sector in facilitating technology transfer—and, thus, proliferation—means the USG must adapt in order to identify, disrupt, and ultimately shut down illicit procurement networks. Adaptation in this environment does not only entail employing conventional tools in a different way or at a different pace. It also means adding new tools, reassessing how various stakeholder groups should relate to one another, and making sometimes difficult decisions about how to reach that end-state.

Moving beyond direct government enforcement, and finding complementary models of industry self-regulation, is essential to prevent proliferation. To be sustainable, those models will need to accommodate the private sector's profit motive; the modern-day Oerlikon, professing a "corporate goal of actively supporting a policy of non-proliferation [that] has priority over commercial interest… [w]ithout prejudice to the legal permissibility of a specific transaction," is the exception that proves the rule.[166]

Accordingly, government will need to fashion incentives that elicit meaningful and durable industry support for its security objectives. That in turn requires that government enhance its knowledge of the economic and political landscape of relevant industry sectors, including the many "facilitators" positioned at key points throughout the physical and informational infrastructure that enables global trade. Only then can government identify how best to leverage the market in support of proliferation prevention. To be sure, the USG will never be able to innovate—organizationally, statutorily, or otherwise—at the speed of 21st-century commerce. Its efforts to respond more flexibly to market realities are bound to remain imperfect, always demanding reappraisal. But by moving to widen its circle of industry interlocutors and recognizing the fundamental importance of well-targeted, market-based incentives, the USG will come closer to an effective counter-trafficking posture.

---

[164] For background on RightShip, see http://site.rightship.com/default.aspx.

[165] Development of the Cybersecurity Framework is being led by the National Institute of Standards and Technology, pursuant to Executive Order 13636, "Implementing Critical Infrastructure Cybersecurity" (February 12, 2013). See http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

[166] Oerlikon Leybold Vacuum, "Export Control Directive" (February 24, 2009). Online at http://isis-online.org/uploads/conferences/documents/Export_Control_Directive_2009.pdf.

About the Managing Across Boundaries Initiative

The Managing Across Boundaries Initiative works to address an increasing array of transnational challenges—from WMD proliferation and the global drug trade, to contemporary human slavery, small-arms trafficking, and counterfeit intellectual property—by looking for innovative government responses at the national, regional, and international levels, and for smart public-private partnerships to mitigate these threats. Our experts and researchers work to conceptualize and catalyze whole-of- society solutions to the most pressing transnational challenges of our day.

About the Stimson Center

Founded in 1989, the Stimson Center is a nonprofit, nonpartisan institution devoted to enhancing international peace and security through a unique combination of rigorous analysis and outreach.

The center's work is focused on three priorities that are essential to global security:

- Strengthening institutions for international peace and security.
- Building regional security.
- Reducing weapons of mass destruction and transnational threats.

The Stimson Center's approach is pragmatic—geared toward providing policy alternatives, solving problems, and overcoming obstacles to a more peaceful and secure world. Through in-depth research and analysis, we seek to understand and illuminate complex issues. By engaging policymakers, policy implementers, and nongovernmental institutions as well as other experts, we craft recommendations that are cross-partisan, actionable, and effective. The center is honored to have received the 2013 MacArthur Award for Creative and Effective Institutions.

Online at www.stimson.org.